March 25, 2016

Via FCC Electronic Comment Filing System

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street SW, Room TW-A325
Washington, DC 20554

Re: Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System (PS Docket No. 15-94) and Wireless Emergency Alerts (PS Docket No. 15-91).

Dear Marlene H. Dortch:

I would like to comment on Notice of Proposed Rulemaking (FCC 16-5) regarding the Emergency Alert System (EAS) in PS Docket No. 15-94 and Wireless Emergency Alerts in PS Docket No. 15-91.

The enclosed document includes my comments in several areas:

1. Highlights from my comments
2. Errata and technical corrections to the current Part 11 – Emergency Alert System
3. Comments on improving alerting organizations
4. Comments on Live Code Tests
5. Comments on technological advances in alerting
6. Comments on securing the EAS

Some of the comments are complex, indicating how difficult some items would be to implement. That shouldn't be taken as a recommendation to implement overly complex solutions.

If you have any questions concerning these comments, please do not hesitate to call (703-892-1810) or email (sean@donelan.com) me.

Respectfully submitted,

Sean Donelan

Enclosure

Re: Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System (PS Docket No. 15-94) and Wireless Emergency Alerts (PS Docket No. 15-91).

Contents

Table of Figures

Works Cited

Arbitron Inc. (2005). *Riding Out the Storm: The Vital Role of Local Radio in Times of Crisis.*

Areospace Defense Command. (1976). Emergency Broadcast System Briefing. In *Emergency Broadcast System (EBS) Procedures* (p. Annex J to ADCOM EBS Procedures). Department of Defense. Retrieved from https://www.fordlibrarymuseum.gov/library/document/0204/7348018.pdf

Canadian Radio-television and Telecommunications Commission. (2014, August 29). Amendments to various regulations, the standard conditions of licence for video-on-demand undertakings and certain exemption orders - Provisions requiring the mandatory distribution of emergency alert messages. *Decisions, Notices and orders*(2014-85). Retrieved from http://www.crtc.gc.ca/eng/archive/2014/2014-444.htm

Chemical Stockpile Emergency Prepardness Program. (2015). *Guide to Implementing the Integrated Public Alert and Warning System (IPAWS).* Department of Homeland Security. Retrieved from https://www.cseppportal.net/Training%20Documents/IPAWS_HowToGuide_21JUL2014.pdf

Clark, D. D. (1988, August). The Design Philosophy of the DARPA Internet Protocols. *Computer Communication Review* , pp. 106-114.

EAS-CAP Implementation Guide Subcommittee. (2010). *ECIG Recommendations for a CAP EAS Implementation Guide (ECIG-IG-1.0).* EAS CAP Industry Group - ECIG. Retrieved from http://www.eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf

Federal Communications Commission. (1994). Report & Order and FNPRM (Establishment of EAS). *FCC Record, Vol. 10*(No. 4), pp. 1786-1901.

Federal Communications Commission. (1995). Memorandum Opinion and Order (Exemption for FM Translators). *FCC Record, Vol. 10*(No. 22), pp. 11494-11506.

Federal Communications Commission. (2015). Part 10 - Commercial Mobile Alert System. *Code of Federal Regulations, Title 47 - Telecommunication*.

Federal Communications Commission. (2015). Part 11 - Emergency Alert System. *Code of Federal Regulations, Title 47 - Telecommunication*.

Federal Emergency Management Agency. (2011). *An Emergency Alert System Best Practices Guide - Version 1.0.* Department of Homeland Security. Retrieved from http://www.fema.gov/pdf/emergency/ipaws/eas_best_practices_guide.pdf

Federal Emergency Management Agency. (2015). *Template: Emergency Communications Plans and IPAWS.* Department of Homeland Security.

Government Accountability Office. (2013, April). Emergency Alerting: Capabilities Have Improved, but Additional Guidance and Testing Are Needed. *Report to Congressional Requestors, GAO-13-375*. Retrieved from http://www.gao.gov/assets/660/654135.pdf

Internet Engineering Task Force. (1989, October). Requirements for Internet Hosts -- Communication Layers. *Request for Comments Series, RFC1122*. Retrieved from https://tools.ietf.org/html/rfc1122

Media Security and Reliability Council. (2005). *Guide to Developing an EAS Public Warning Plan to Serve Local Areas.* Retrieved from http://www.mediasecurity.org/documents/EAS_Appendix.pdf

National Academy of Sciences. (2003). *The Internet Under Crisis Conditions: Learning from September 11.* National Academies Press . Retrieved from http://www.nap.edu/catalog/10569/the-internet-under-crisis-conditions-learning-from-september-11

National Computer Security Center. (1983). *Trusted Computer System Evaluation Criteria ("Orange Book").* Department of Defense.

National Institute of Standards and Technology. (2008, July). Guide to General Server Security. *800-123*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

National Institute of Standards and Technology. (2015, May). Guide to Industrial Control Systems (ICS) Security. *NIST Special Publication, 800-82 Rev.2*. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

National Weather Service. (2004, April 14). Western Region Proecedures for Incorporating Direct Audio Access All-Hazards Messages on NOAA Weather Radio. *NOAA Weather Radio (NWR) Dissemination, NWSI 10-1710*(WR Supplement 3-2004). Retrieved from http://www.nws.noaa.gov/directives/sym/pd01017010w032004curr.pdf

National Weather Service. (2011, October 3). NOAA Weather Radio (NWR) All Hazards Sepcific Area Message Encoding (SAME). *National Weather Service Instruction, NWSI 10-1712*. Retrieved from http://www.nws.noaa.gov/directives/sym/pd01017012curr.pdf

Office of Telecommunications Policy. (1974). *Emergency Broadcast System Procedures Manual.* Executive Office of the President. Retrieved from https://www.fordlibrarymuseum.gov/library/document/0204/1511749.pdf

Office of the U.S. Attorneys. (2009). *U.S. Attorney's Manual.* Department of Justice. Retrieved from https://www.justice.gov/usam/united-states-attorneys-manual

Public Safety and Homeland Security Bureau. (2013). *Strengthening the Emergency Alert System (EAS): Lessons Learned from the Nationawide EAS Test.* Federal Communications Commission. Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/DOC-320152A1.pdf

Re: Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System (PS Docket No. 15-94) and Wireless Emergency Alerts (PS Docket No. 15-91).

Society of Cable Telecommunications Engineers. (2013, October). Emergency Alert Messaging for Cable. *CEA/SCTE Standard, J-STD-42-B, SCTE 18:2012*.

Re: Amendment of Part 11 of the Commission's Rules Regarding the Emergency Alert System (PS Docket No. 15-94) and Wireless Emergency Alerts (PS Docket No. 15-91).

1. Executive Highlights

The Notice of Proposed Rule Making FCC 16-5 is an inquiry into a broad range of Emergency Alert System topics. I would like to highlight a few items, which are covered in more depth later.

1. An update or new interpretation of the essential White House statement of requirements for EAS is needed. The concept of seizing all mass media channels for indefinite periods of time carried over from EBS to EAS has been, although not always recognized as such, a contributing factor in several disruptive EAS incidents. During a national catastrophe, a brief alert on all channels the President is about to speak would likely be enough to prompt the public to seek out those mass media outlets still operating and carrying the Presidential message; without the problems indefinite length channel seizures cause.
2. The Key Performance Indicators for the EAS should be from the point of view of the public, not the government or industry. Instead of saying the EAS interrupts a program channel and transmits a message, the EAS notifies the public (viewer, listener, audience, etc.) How quickly does the public successfully receive the correct information affecting them? The National Weather Service may transmit tens of thousands of EAS messages, but effectiveness should be measured by how many relevant messages reach how many affected people? How often is the public interrupted by irrelevant messages, or incomprehensible messages? Six separate “targeted” alerts which interrupt programming across a large population area may be more disruptive than a single broad alert for the same population area even if it is less “targeted.” On the other hand, that 1 warning may have been critical to that person but they couldn’t understand it or didn’t receive it.
3. The burden of maintaining EAS plans and operations should be distributed across a broader range of entities, both government and industry. This would reduce volunteer burn-out and ensure the appropriate entity is responsible for maintaining their own portion of EAS plans and information. Expecting volunteers to coordinate uncooperative or disinterested entities is not realistic.
4. New technologies should enable individual choice and control about which alerts interrupt the individual’s activities, recognizing that EAS is a mass media communication channel. Individuals should be able to opt-out of most alerts. Only the minimum number of critical alerts should always notify the individual but still allow dismissing the warning. System testing should be frequent, but shouldn’t disrupt the public’s activities, unless an individual opts-in to system tests.
5. Ambiguities in the EAS protocol and lack of published Federal EAS operational plans hinder alert validation and verification. Confusion about which sources could issue which messages, and how means recipients can’t predict or automatically sanity check them. Current plans and operational handbooks don’t contain procedures for handling false alerts or other EAS contingencies. They assume everything works correctly.

6. Manufacturer default security configurations are crucial to the operational security of the EAS. Expecting the buyer or operator to secure the configuration after they purchase has not worked for other software, automobiles or anything else. Manufacturer certification must include testing the security of EAS equipment, including reasonable red-teaming/penetration testing by an independent agent. This will increase manufacturer costs, which will be passed along to customers someway. Patches are part of the software life-cycle, and not a one-time event. On-going equipment maintenance will be necessary.
7. Only specific tactical information needs to be confidential in EAS operational plans. Most sections of EAS operating plans should be published, and the tactical details placed in a confidential appendix. Because tactical information often needs updating, keeping the tactical information in a separate appendix makes that easier. Government warning information should be considered public information. Restricting warning sources to only members of industry groups limits new entrants and hinders system improvements; as well as defeating the purpose of government warnings keeping the public informed.
8. In addition to the topics the FCC asked about, EAS equipment certifications and system operations should include robustness testing, as well as current verification testing. Asserting that operators shall never make a mistake doesn’t actually prevent or fix a problem. More testing and training alone won’t solve all the problems. FEMA, FCC and NWS, as joint responsible agents for the EAS, should proactively look for and address potential problems in the policies, protocols, equipment and operations.

2. Errata and Technical Corrections

Minor printing or technical errors should be corrected in Part 11 – Emergency Alert System (EAS). While occasional editing and printing errors occur in all documents, they are usually corrected the next edition or printing. FCC did this in Appendix 1: Rule Clarifications as part of its Memorandum and Opinion (Exemption for FM Translators) (Federal Communications Commission, 1995).

Some of the current printing and technical errors in the annual printed editions of the Code of Federal Regulations, 47 CFR Part 11, (Federal Communications Commission, 2015) include:

> § 11.31(c) Since 2012, the second repetition of the example EAS header contains a lowercase "p" between "TTTT" and "JJJHHMM" instead of a hyphen "-". The message format in all three repetitions of the EAS header should be identical.
>
> § 11.31(f) Since 2003, the table of State, Territory and Offshore ANSI number codes (SS) repeats ANSI number "68" (Republic of the Marshall Islands - MH) and omits ANSI number "69" (Commonwealth of the Northern Mariana Islands - MP). The table should include each ANSI code once. Or incorporate by reference the ANSI, Census and National Weather Service sources.

3. Improving Alerting Organization at the State and Local Levels

A successful public alerting system at the state and local levels involves a combination of groups. The FCC has traditionally focused on:

- Federal, State and local government officials
- FCC mass media license holders (EAS participants)

In addition, the following groups affect how well the system keeps the public informed:

- Private (non-mass media) communications industry (telephone/internet, microwave/satellite distribution networks, EAS/CAP aggregator service companies, etc.)
- Broadcast/industrial electronics manufacturers (EAS devices, content management systems, etc.)
- Private mass notification systems at schools, industrial sites, etc.
- Consumer electronics manufacturers (smart phones/devices, weather radios, etc.)
- Consumer software/application creators (mobile apps, desktop apps, etc.)
- Other consumer entertainment and information organizations (radio/TV networks, Internet entertainment subscription services, etc.)

Including all the parties, and distributing the workload will also help avoid volunteer burn-out.

3.1. EAS Designations

Terminology is important for people to understand how a system works, but the names don’t necessarily change how a system actually works. As William Shakespeare wrote " What's in a name? that which we call a rose by any other name would smell as sweet." Changing terminology tends to have ripple effects as other documentation needs to be changed or, as often happens, just not updated. For example, the U.S. Attorney’s Manual (Office of the U.S. Attorneys, 2009) still references the term “Common Program Control Station (CPCS-1)”.[1] Whatever name the U.S. Attorney’s Manual uses probably will not affect a U.S. Attorney’s ability to meaningfully review a case. It may create some extra work for them versus making extra work for someone else. When it is necessary to change terminology, it should not be surprising that cross-references will be needed between the old and new words.

3.1.1. Roles and Designations

EAS designations help EAS participants understand which sources could carry which messages, and help government originators understand which EAS participants to contact. Nevertheless, messages will travel based on the actual connections, regardless of the names, colors or technology of the connections.

[1] http://www.justice.gov/usam/criminal-resource-manual-1669-destruction-government-property-application-section-1362

When FEMA distributes the same nation-wide messages through PEP stations, all PEP sources are interchangeable. However, if FEMA distributes both nation-wide and regional-coded messages, e.g. a nation-wide Emergency Action Notification (EAN) and a follow-up regional National Information Center (NIC) message, different PEP and NP sources could carry different subsets of national messages. Would PEP and NP stations need to identify a particular state/region, e.g. NP (Virginia) or PEP (FEMA Region VIII)?

Some state EAS plans have cross-border EAS areas, but the multi-state nature of modern satellite, IPTV and large cable networks isn't reflected in EAS state-based designations. Broadcast stations rarely monitor EAS sources more than 70 miles away. Satellite, large cable head-ends, and IPTV video hub offices often extend across several states, and may monitor a NP station from several states away. Sirius XM, Premiere Networks and NPR National squawk channel for EAN distribution is an example of inter-state relay networks (IRN), which aren't strictly part of any state plan. Affiliates of those satellite services could be designated in state EAS plans as National Relays (NR) of national messages. Satellite TV providers don't carry state/local messages, except as pass through on local broadcast channels. They could be designated NR-only providers.

Because different levels of relay networks act as a source for different levels of messages (national, state and local); using a single designation like Relay Station (RS) may be confusing below the national level.

Some EAS participants play a dominant role in their markets independent of their role in EAS distribution. However, market dominance can change based on mergers, bankruptcies and the fickle nature of markets. Market dominance should not be reflected in EAS designations. FCC may want to develop a separate risk management profile, which could change based on the marketplace. It would be very difficult for volunteers to keep such an analysis up to date.

Common Alerting Protocol (CAP) distribution is currently related, but independent of EAS Protocol distribution designations. CAP messages are distributed via a parallel network. Essentially all EAS Participants are CAP clients of CAP gateways. CAP gateways and aggregators are currently government funded and/or operated.

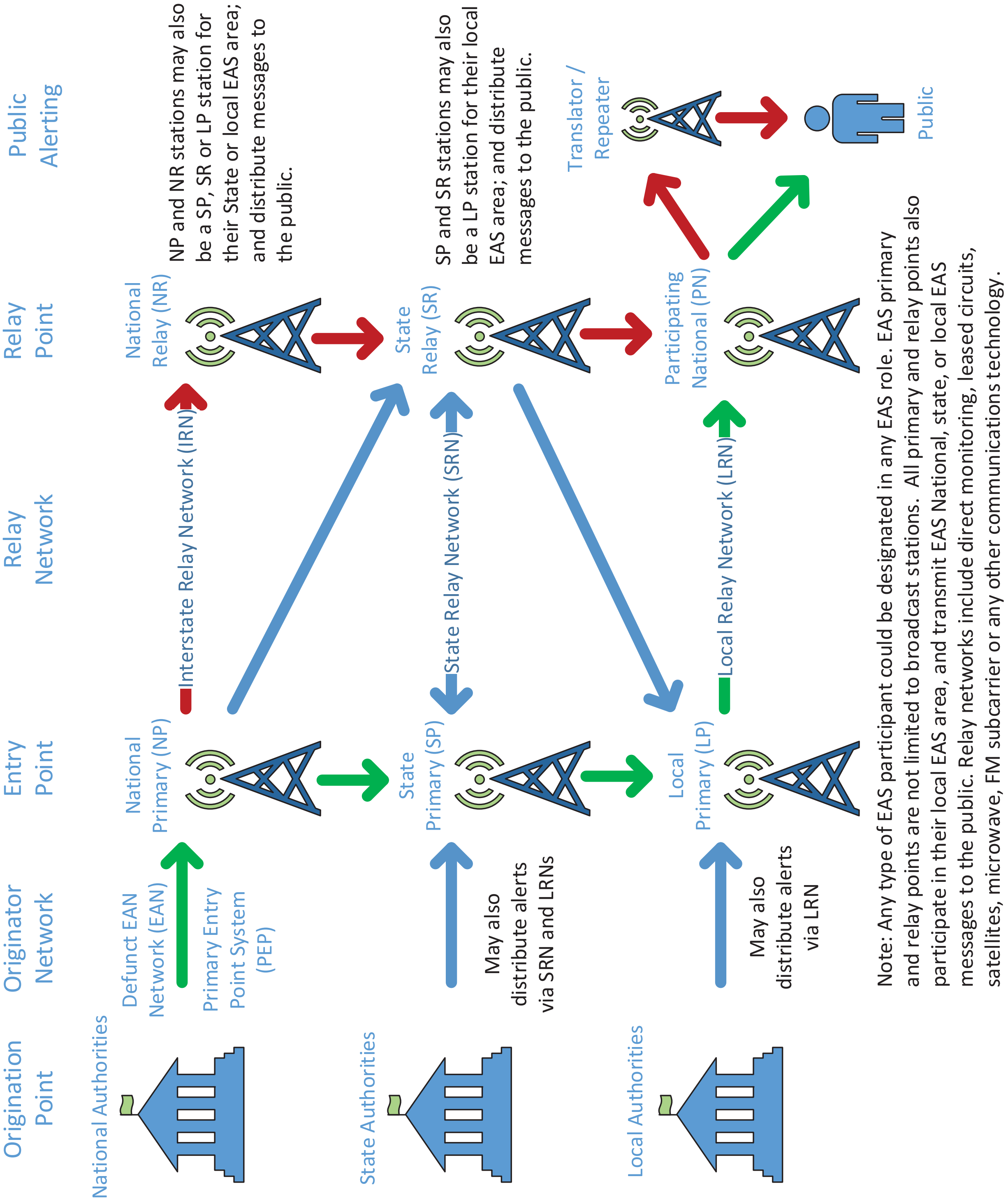
In Table 1, I propose a taxonomy of EAS roles, adding a few new designations and clarifying existing designations. The EAS roles and designations are outlined with heavy-borders.

Role	**Designation**	**Explanation**
Origination Point (Government)	FEMA, NWS, State/local EMAs President, Governor, Mayor	National, state and local authorities responsible for issuing official alerts and warnings (e.g. government officials and emergency communication centers). In rare cases, a government agency may designate specific non-government originators, such as nuclear power plants.
Originator Network (Government)	PEP, EDIS, POTS, FAX, P25, etc.	Closed circuit networks (e.g. telephone, radio, satellite, etc.) funded by government agencies connecting government Origination Points to EAS Entry Points. Some states and local governments also fund and operate Relay Networks, i.e. combines an Originator Network and a Relay Network connecting some or all EAS participants in an area.
Entry Point (Licensee)	National Primary (NP) State Primary (SP) Local Primary (LP)	Acts as the industry Point of Contact for government originators requesting activation of the Emergency Alert System. Accepts the message, and if necessary prepares the audio recording and EAS header codes. It initiates the EAS transmission to downstream Relay Networks, Relay Points, and the Public. Usually requires staff at the Entry Point, unless the government originator maintains and uses its own EAS-compatible equipment.
Relay (Mid) Network (Mass media and private networks)	Interstate Relay Network (IRN) State Relay Network (SRN) Local Relay Network (LRN)	Relays EAS messages between distant Entry Points and Relay Points. It may be a combination of closed-circuit networks and EAS participant public transmissions. Usually funded by industry participants, so cost is kept to a minimum using mostly over-the-air monitoring. Optional when direct monitoring is possible between Entry Points and Relay Points.

Relay (Exit) Point (Licensee)	National Relay (NR) State Relay (SR) Participating National (PN)	Source of EAS messages from, but not the Point of Contact for, government originators for downstream Entry Points (i.e. National to State to Local) and local Participating National (PN) stations. All Entry Points (NP, SP, LP) and Relay Points (NR, SR) also participate in their state/local EAS areas, i.e. act as Participating National (PN) stations relaying EAS national, state and local messages to the Public.
Public Alerting	Translator/Repeater The Public	Re-transmits messages to the Public or group, includes non-licensed private, campus and industrial alerting systems. The purpose of the Emergency Alert System – informing the Public.

Table 1 EAS Roles and Designations

In Figure 1, I show a (greatly) simplified EAS distribution daisy-chain with EAS roles. For graphic convenience, I used only broadcast towers. But any type of EAS participant can serve in those roles.



NP and NR stations may also be a SP, SR or LP station for their State or local EAS area; and distribute messages to the public.

SP and SR stations may also be a LP station for their local EAS area; and distribute messages to the public.

May also distribute alerts via SRN and LRNs

May also distribute alerts via LRN

Note: Any type of EAS participant could be designated in any EAS role. EAS primary and relay points are not limited to broadcast stations. All primary and relay points also participate in their local EAS area, and transmit EAS National, state, or local EAS messages to the public. Relay networks include direct monitoring, leased circuits, satellites, microwave, FM subcarrier or any other communications technology.

Figure 1 EAS Roles and Daisy-Chain Distribution

3.2. State EAS Plan Filing Interface (SEPFI)

The advantage of paper-based plans and forms is easy handling of exceptions and unique conditions. Ad hoc changes can easily be written on the paper. The disadvantage of paper-based plans and forms is data quality and consistency. Electronic forms can improve data quality, but require more extensive pre-planning and field testing. Simply scanning paper documents and uploading to a web site is not an electronic form. Exceptions and unique conditions are more difficult to handle with electronic forms. A well implemented electronic filing system for EAS data will be very useful for analysis of EAS and reduce the burden on state and local EAS committee volunteers.

It is not clear from the description of the State EAS Plan Filing Interface (SEPFI) whether it is limited to the data needed to populate an EAS Map book; or it is intended to include all parts of a State EAS plan. The EAS Map book is primarily a database, similar to other FCC license databases like the media bureau’s Consolidated Database System (CDBS) and Cable Operations and Licensing System (COALS), and the wireless bureau’s Universal Licensing System (ULS). On the other hand, the FCC online Public Inspection Files is primarily an online document storage system.

3.2.1. Structure

The Chemical Stockpile Emergency Preparedness Program (CSEPP) has prepared several model plans. Because participation in state and local EAS plans is voluntary, and even which emergency event codes an individual EAS Participant chooses to transmit, the CSEPP includes model EAS surveys to collect information from EAS Participants (Appendix D, Guide to Implementing the Integrated Public Alert and Warning System (IPAWS)). Just because a state or local EAS plan includes specific event codes doesn’t mean any EAS participants have configured their EAS equipment to automatically or manually carry those emergency messages.

How EAS Participants and monitoring sources are identified will depend on the available database information. Using various database primary keys, such as the CDBS Facility ID and COALS Physical System ID, makes linking correct records together easier and keeping the information up to date. However, database primary keys are generally less user friendly. Humans use call letters, community names, and company brands because they are easier for humans to remember.

The online user interface should include user tools, such as drop-downs, search boxes, maps, etc.; to help the EAS Participant find the available key EAS sources for their location and automatically fill in the appropriate details. CDBS and COALS have some data quality issues and some data fields are not suitable for linking, e.g. Community of License is usually a city name but is sometimes an aspirational location. Different counties may have cities with the same name. All FCC databases should improve data quality by cross-referencing data fields with authoritative sources, such as US Postal Service for mailing addresses; US Census and USGS for spelling of States, counties and places; USGS for a longitude/latitude within the boundary of a State, county or place; other FCC licensing databases, and other data quality checks.

Key EAS monitoring sources should be designated and curated by the appropriate organization. For example, FEMA should be responsible for curating the list of PEP/NP sources, NWS should be responsible for maintaining the list of Weather Radio sources, SECCs should be responsible for curating the list of State Primary and Relay sources within their states, LECCs should be responsible for curating the list of Local Primary sources within their Local EAS area, FCC/FEMA should be responsible for curating the list of non-geographic/nation-wide EAS sources. Various unique distribution systems and CAP aggregators should be curated by their respective sponsors, e.g. SECC if it is an industry operated state relay network, the State EMA if it is a state operated network, FCC if it is an inter-state relay network, FCC for IPAWS, etc. Based on state EAS plans and other information on state broadcast association web sites, approximately 25 states use only over-the-air broadcast stations for state distribution, and 25 also use other distribution channels (satellite, telephone, microwave, state radio/TV closed-circuit network, or small enough for direct reception).

Individual EAS Participants should maintain their own records, and select their key EAS sources from the previous curated lists for their location. In most cases, the default key EAS sources for their Local EAS Area will be selected. If an EAS Participant requires an exception because they can’t receive one of the curated key EAS sources, the SEPFI could include a workflow process for approval, or just allow the EAS Participant to specify an alternative monitoring source. Additional EAS details may be collected, such as supplementary EAS sources monitored, counties/sub-counties/communities included in the system service area, and which event codes they relay.

3.2.2. Security

Over 40 states publish their EAS plans. The remaining states and territories haven’t published their EAS plans because of confidentiality, don’t have a plan, can’t afford a web site, or no particular reason. Information about public broadcasters, such as call signs, locations, ownership is available in several FCC databases and other public sources. Consolidating state EAS plan information with the FCC would make it subject to the Freedom of Information Act. SECCs/LECCs often don’t have a legal existence, and therefore may not have public disclosure requirements.

The most cost-effective way to protect potentially sensitive information is not to collect it.

The most sensitive information in State EAS plans is generally the authorization codes and EAS activation contact information such as non-published telephone numbers of station control rooms and state emergency operation centers. This is different than the administrative contact information such as the list authorized government officials and official telephone numbers. It should not be necessary for the SEPFI to collect sensitive tactical information, such as authorization codes and non-published telephone numbers used to activate the EAS. SECCs/LECCs should distribute that information directly to those with a need to know, such as the state emergency operation center and state primary sources. The SEPFI should collect the administrative information, e.g. government agency, job title, etc. for the list of officials authorized to request EAS activation.

Most other information in state EAS plans shouldn't require confidentiality. Even states without published EAS plans, publish the list of EAS areas, key EAS sources for the state and each local area, monthly schedule for tests, etc. Most SEPFI security concerns will involve the integrity of the data and availability of the system. Because SEPFI may not be accessible during an emergency, EAS Participants, and other systems which use EAS information, will need to download and save copies of the State EAS Plans and associated information. Excessive confidentiality controls on SEPFI will hinder its use during an emergency. Integrity controls must be in place to audit who made what change and when.

3.2.3. National Advisory Committee (NAC)

The EAS has expanded beyond the classic broadcast industry. A modern National EAS advisory committee should include representatives from all types of EAS Participants and state/local government stakeholders. The Media Security and Reliability Council and National Security Telecommunications Advisory Committee had more representative industry participation.

3.3. State EAS Plan Contents

The EAS and planning is a joint and cooperative responsibility of Federal (FEMA, FCC, NOAA NWS), State and local levels of government and industry. The burden must not fall solely on a group of industry volunteers. The FCC must also accept its own responsibilities and contribute resources and personnel to assist in State and local planning and follow-up assistance. The former Emergency Broadcast System included memorandums of understanding between industry and FEMA, FCC and NOAA which outlined agency responsibilities and cooperative effort for developing EBS plans and capabilities at State and local levels.

The Media Security and Reliability Council published a "Guide to Developing EAS Public Warning Plan to Serve Local Areas" in 2005. It outlines the major topics which should be included in every EAS plan.

3.3.1. Organizational Elements

The national, state and local EAS plans and operating procedures collectively make up the "National Emergency Alert System Plan." This includes all of the following: the national control point procedures, national EAS operating handbooks, state and local plans, and map books. The duties and burdens of maintaining parts of the EAS plan should be distributed and coordinated between several entities, including industry volunteers, EAS Participants, national, state and local government agencies.

EAS Plan Topic	National	State	Local

A list of the EAS header codes and messages that will be transmitted by key EAS sources	FEMA	State EMA, NWS	Local EMA, NWS
Procedures to transmit emergency information to the public during an emergency using EAS	FCC, FEMA, PEPAC, Non-geographic / Nation-wide EAS Participants, EAS Equipment manufacturers	State EMA, NWS, SECC, State-wide EAS Participants	Local EMA, NWS, LECC, Local EAS Participants
A data table, in computer-readable form, clearly showing monitoring assignments	FEMA, PEPAC, National Primary and Relay (PEP/NP/NR) sources, unique distribution channel providers, Non-geographic / Nation-wide EAS Participants	NWS, SECC, unique distribution channel providers, State Primary and Relay (SP/SR) sources, State-wide EAS Participants	NWS, LECC, unique distribution channel providers, Local Primary and Participating (LP/PN) sources, Local EAS Participants
A description of how CAP-formatted messages will be aggregated and distributed to EAS including the monitoring requirements	FEMA IPAWS	State EMA, NWS, SECC, CAP Aggregators	Local EMA, NWS, LECC, CAP Aggregators
Unique methods of EAS message distribution	FEMA, NPR, Premiere Networks, Sirius XM, Unique Distribution Channel Providers	State EMA, SECC, Unique Distribution Channel Providers	Local EMA, LECC, Unique Distribution Channel Providers
Instructions for activations of EAS, including a list of all authorized entities participating in EAS	FCC, FEMA, National Control Point Procedures, National Primary (PEP/NP) sources	State EMA, NWS, SECC, State Primary (SP) sources	Local EMA, NWS, LECC, Local Primary (LP) sources

Procedures for conducting EAS tests	FCC, FEMA, PEPAC, EAS Equipment manufacturers, PEP/NP sources	State EMA, NWS, SECC, CAP Aggregators, SP sources	Local EMA, NWS, LECC, CAP Aggregators, LP sources

Table 2 EAS Plan Topics and Responsible Entities

State Emergency Communications Committee Governance Structures are basically voluntary organizations, often nothing more than an informal gathering of interested parties, and sometimes just a single person doing all the work. There is nothing which can be held responsible. Fining or punishing volunteer groups just leads to no one volunteering to participate in those groups. Unless the FCC or other government agencies intend to fund the operations of SECC/LECC organizations, it has limited power to force them to perform specific duties. Current state and local EAS plans are only updated when and if volunteer resources are available. Most of the time, SECC/LECC groups are begging for additional volunteers when current members retire or pass away. Even the FCC decided it didn't have the resources to maintain national map books, update its EAS Operating Handbooks or review and approve State EAS plans for years.

The activities of governmental agencies, such as FCC, FEMA, NWS, State and local Emergency Management Agencies (i.e. first responders, law enforcement, emergency communication centers, etc.) are not under the control of SECC/LECC volunteer organizations. SECC and LECC industry volunteers are experts in their specific industry practices, mostly broadcast engineers but also some other communication technologies, and are not necessarily expert emergency managers or planners. Public emergency planning and public alerting is an inherent governmental responsibility. Industry is prepared to assist the government in performing some of those duties, but industry should not be expected to coordinate government agencies or make decisions about those inherent governmental public warning responsibilities. SECC membership should include the industry EAS participants, State emergency management agencies, the regional National Weather Service office, the regional FEMA office, and regional FCC office. The Federal agencies could be ex-officio, non-voting members providing assistance to the SECC. In large government agencies, unless that job is explicitly part of someone's duties, it tends to be overtaken by other duties.

A voluntary SECC or LECC can only include in EAS plans the information government agencies choose to share, assuming state/local government agencies choose to participate at all. Instead of duplicating work of creating an EAS plan at each level; and in 50 States, District of Columbia, 5 Territories, and optionally 3 Freely Associated States; plus, approximately 500 local EAS areas;

FCC, FEMA and NWS should fund and assist with the development of a national EAS plan with templates for model State and local EAS plans. Collectively these would work together as a coherent overall EAS plan, operating procedures and instruction handbook. At the state-level (States, District of Columbia and Territories), state officials and state industry volunteers could customize the model State and local plans for unique state requirements and challenges. Likewise, at the local level, local officials and local industry volunteers could customize the model local EAS plan, if needed, for unique local requirements and challenges. Often State and local EAS area plans contain a lot of boilerplate information, and only need to customize the geographic borders of local EAS areas within the state, designate key EAS monitoring sources at the state and local levels, annual testing schedules, and points of contact for government agencies and industry participants.

Instead each entity should be responsible for keeping their portion of the plans, and their contact information up to date instead of requiring volunteers try to get government agencies and industry organizations to respond. Information about unique distribution methods for EAS is often controlled by contracts and agreements between the communication provider and the government agency paying for the system or service, not the SECC or LECC. Information which requires regular updating, e.g. annual testing schedules, changing the names of officials, station call letters, updating contact information and authentication lists would not require plan changes or new approvals.

Local Emergency Communication Committees (LECC) and Local EAS areas depend greatly on local factors, which may be somewhat obvious. The entity that has legal responsibility for local warnings, which may be a regional, county or city government organization, must be identified and be included in the local EAS area governance process. Many local EAS areas tend to operate on auto-pilot with the SECC or local volunteer performing most of the administrative functions with little participation by local government authorities. But some Local EAS areas have a mega-population center, such as New York City; or include a nuclear power plant, chemical stockpile facility or another unique hazard requiring special local EAS procedures. Additionally, LECCs provide a forum for local EAS Participants and local government emergency agencies to pre-coordinate with each other before a crisis. Although the State and local EMAs should already coordinate with each other, it is critical that local industry EAS contacts and local government alerting/warning contacts know each other at the engineering/technical level in addition to the typical reporter/public information officer level. The local LECC should include local government emergency management agencies, the NWS office for the local area, local EAS Participants, as well as representation from nuclear power plants, chemical stockpile facilities, etc. which would require activating the EAS. The SEPFI could include local contact information for various local entities involved with alerting and warning at the local level. This will greatly expand the amount of information being collected.

3.3.2. Operational Elements

The EAS is complementary to other emergency public information and warning systems and plans. State and local EAS plans contain information for activating and operating the Emergency Alert System, not every warning system. State and local emergency management agencies and other government agencies have their own emergency plans, procedures and manuals for alerting the public which cover all the systems they could use for different types of emergencies. State and local EAS industry plans should be written so the State and local government agencies can incorporate, as a chapter or appendix, the relevant EAS activation procedures within the agency's procedures, manuals or plans.

For example, the New York City Office of Emergency Management uses various alerting pathways based on incident severity. The EAS plan should not attempt to cover all of the alternative alerting methods.

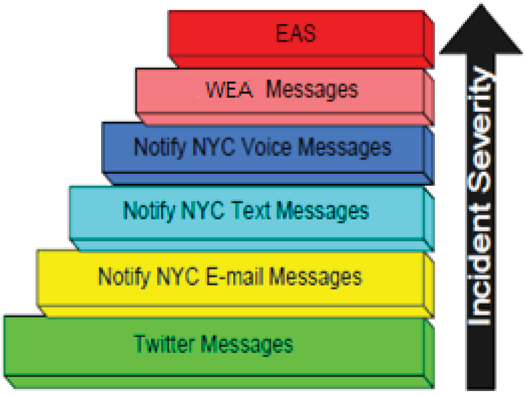


Figure 2 NYC OEM's Communication Pathways Ranked by Severity

3.3.3. Testing/Outreach Elements

As I explain further in section 4.1 Live Code Tests below, I suggest calling these exercises or drills and creating a separate §11.62 for EAS exercises. Because each EAS special test or exercise tends to be semi-unique, the State plan shouldn't include the exercises themselves, but document the process for coordinating and distributing information about the exercise to EAS Participants. The organizer of the exercise should have the primary responsibility for pre-test public outreach, and EAS Participants can assist with those outreach activities.

System testing is important for ensuring the proper operation of the EAS. System testing should frequent, but unobtrusive and minimize public disruption as much as possible. Coordinating required monthly testing of the EAS is the most visible activity of most SECCs/LECCs. While several alerting systems, such as Wireless Emergency Alerts and public warning sirens may provide the public an initial indication of an emergency or Presidential Alert; mass-media communication channels will be the primary source of the actual message. If national plans expect to use the EAS, then it needs regular testing.

Testing and public awareness activities should be considered distinct activities. I suggest updating §11.61 to concentrate on system testing, and making it more consistent across all types of EAS Participants. In particular, system testing on all-types of multi-channel audio and audio/video systems can be accomplished with less public disruption while still ensuring EAS equipment works. I have included some suggested EAS rule language improvements later in this paper.

Using Public Service Announcements and occasional EAS exercises eliminates the need to use required monthly and weekly tests for public awareness education. State and local EAS plans may need an additional section for EAS PSA's. EAS Participants need to run occasional PSA's instead as an alternative way to conduct public awareness and education.

3.3.4. Security Elements

State and Local EAS Area plans describe how the EAS should work. They are not documentation of what EAS Participants have done to comply with any FCC requirements, including their compliance with the proposed FCC security requirements.

State and Local EAS Area plans should describe any state-specific or local EAS area-specific security requirements EAS Participants should implement. This is most likely needed for unique distribution communication channels. Generally, EAS security requirements should be similar at federal, state and local levels; and should be covered by the common National EAS Plan and EAS equipment manufacturer documentation.

Most SECC/LECC groups don't actually own or operate any EAS infrastructure themselves. If the FCC adds extensive confidentiality requirements for EAS plans, contact information and tactical details; SECC/LECC volunteers may be faced with needing background checks, security audits and costly security processes themselves, making an already thankless task even more burdensome.

4. Building Effective Community-based Alerting Exercise Programs

4.1. Live Code Tests

A small suggestion, I suggest using the term “live code drill” or “live code exercise” instead of “test.” Although pedantic, and doesn’t change the action itself, the purpose of these exercises is different than testing the Emergency Alert System. As an analogy, during “fire alarm system testing,” the public is told to ignore the fire alarms. During “fire alarm drills,” the public is encouraged to react and participate in the exercise such as evacuating the building. I understand section 11.61 is called “Tests of EAS procedures,” therefore the FCC calls everything “testing.”

Historically, EAS has conflated testing, exercises and training/awareness. EAS sometimes justifies frequent testing as public awareness. System testing should be frequent, but also unobtrusive or invisible to the public to avoid warning fatigue (the boy who cried wolf). Weekly tests on hundreds of channels at “random” times for training purposes, although most EAS Participants automate the process and don’t use them for training; plus, monthly tests on hundreds of channels has mostly taught the public those data squawks mean change the channel quickly because an obnoxious tone is coming, because in the public’s experience, important information almost never follows the Attention Signal. Imagine if apartment buildings and offices conducted weekly fire alarm tests for “public awareness.” The public would get fed up with those frequent disruptions and noises. Home smoke detectors are now hard-wired, because the public would remove (and never replace) the battery when the detector beeped at 3am in the morning. No matter how important officials think something is, the public always makes the final decision whether or not it’s important to them.

Exercises/drills involving the public are usually less frequent for that reason. For example, a hypothetical state/local EAS testing and exercise annual schedule could be the following:

Month	**Time**	**Level**	**Originator**	**Entity**	**Protocol**
January	Daytime	Local	EAS	Local Primary	EAS
February	Nighttime	Local	CIV	Local EOC/EMA	CAP
March	Daytime	Local/State	CIV or NWS	***Spring Live Code Drill***	EAS/CAP
April	Nighttime	Local	CIV	Local EOC/EMA	EAS
May	Daytime	State	EAS	State Primary	EAS
June	Nighttime	State	CIV	State EOC/EMA	CAP
July	Daytime	Local	CIV	Local EOC/EMA	CAP
August	Nighttime	Local	EAS	Local Primary	EAS
September	Daytime	Local/State	CIV or NWS	***Fall Live Code Drill***	EAS/CAP

October	Nighttime	Local	CIV	Local EOC/EMA	EAS
November	Daytime	National	PEP	FEMA PEP/NP	EAS/CAP
December	Nighttime	State	CIV	State EOC/EMA	EAS

Table 3 EAS Exercise and Testing Schedule

In most local building fire codes for ordinary office occupancies, fire drills should be conducted once or twice a year. While the number of allowable EAS Live Code Drills will always be somewhat arbitrary, between quarterly and annually is probably the appropriate number. Just as important is adjacent jurisdictions should coordinate EAS Live Code Drills to avoid too many within a short time frame in cross-border EAS local areas. If the FCC does not put limits on the number of allowable EAS Live Code Drills; the public should be informed which government agency/agencies to complain about frequent drills

Using the CAP EASText element or ECIG constructed Alert Text as specified in the “CAP EAS Implementation Guide” (EAS-CAP Implementation Guide Subcommittee, 2010) instead of the translation of the EAS Header codes would reduce the opportunity for confusion during Live Code Drills. The EASText or Alert Text enables message authors to include vital details, such as “this is a test,” and keep the audio and video crawl consistent. The local translation of the EAS Protocol Header Codes should not be required when using EASText or Alert Text from the CAP information. Multi-lingual alerts have language specific EASText elements or elements for the Alert Text created by the alert originator to keep the audio and video crawl consistent, requiring the EAS Header Code text defeats that purpose. Computer translated text may create undetected dangerous errors. Messages relayed using the EAS protocol or through classic EAS devices would still display a video crawl using the EAS Header code translation.

5. Leveraging Technological Advances in Alerting

5.1. Background and Technological Changes Since 1994

Technology has continued to change. In some sense some issues have gotten both better and worse. It has gotten better because digital systems have more alternatives. It has gotten worse because the world is a mixed up mess of different types of systems.

The original design of the CONELRAD and Emergency Broadcast System was based on distributing a common emergency message through broadcasters in a local operational area. In theory, because all broadcasters and cable systems in the local EAS area carry a common emergency message, the source of the common emergency message and distribution channels of the common emergency message wouldn't matter. In practice, different EAS Participants choose to carry different emergency messages. Each participant decides which emergencies are worthy of news coverage. In most areas, only a very small, minority of EAS Participants consider any EAS messages, beyond the required EAN, worthy of disrupting programming. Even EAS Participants with news departments may decide a local emergency at the outer edge of their service areas is not important enough to cover as breaking news, and may decide to cover it later during their normally scheduled newscast. These are normal news editorial judgements of an independent press.

The original design for EAS was not intended for hyper-local emergency messages. Local EAS Areas are regional sized areas, usually containing multiple counties, sometimes crossing state borders. There are a few exceptions, such as New York City is large enough to be its own local EAS area covering several counties. In general, counties, cities and local municipalities were encouraged in EBS and EAS plans to coordinate with state/regional organizations because EAS interrupted and disrupted the public throughout a large region. For example, in April, 2014, there was a multi-state 911 outage. Multiple Public Safety Answering Points independently activated the EAS in several local EAS areas, and sometimes the same local EAS area multiple times, resulting in multiple programming interruptions of EAS Participants and annoying some members of the public based on Twitter messages. Although each PSAP only intended to notify the public within their jurisdiction, EAS areas, radio waves and cable systems do not stop at political boundaries. In almost every state, EAS activations bleed over into adjacent states; which means the FCC and FEMA should act in a coordination role even for intra-state EAS actions in addition to national messages.

While the old view of subscription multi-channel programming services was they didn't cover local emergencies; in some cases, cable channels now originate local news, including breaking news and emergency coverage. On the other hand, several radio and TV stations have changed to completely automated operation, and are unattended much of the time. They are now programmed via satellite or computer delivered programs with no local coverage during local emergencies. Some broadcast radio and Digital TV stations are also re-transmitting other broadcast stations, such as an AM radio news station on a FM HD-2 or FM HD-3 digital channel. The FM station may be carrying automated programming on its primary audio channel HD-1, while the HD-2 channel carries a re-broadcast of an AM news station with breaking news coverage. Assumptions based on the category of an EAS Participant are no longer accurate.

University campuses and military bases have installed mass notification systems which interrupts a university broadcast radio and TV station using EAS, and all channels on multi-video programming systems in the university campus dorms or military base housing. In most cases university campus and military base MVPD systems are considered Satellite Master Antenna TV (SMATV) systems or Private Cable Operators (PCO), and not covered by EAS Part 11 rules. Although university campus and military bases are not required to implement EAS on the SMATV/PCO systems, the hyper-local nature of their emergency alerts makes sense for them to override all broadcast, satellite and campus origination channels for on-campus or on-base emergencies. In small community franchise MVPD systems, it may also make sense to override other regional programming, including broadcast stations, with hyper-local emergency information. The hyper-local alert is likely to impact and be of concern to the public within that single community. But when a MVPD system serves a large region with multiple communities, such as a MSO, DBS or SDARS, it may make sense not to override regional sources of emergency information with hyper-local emergency information. A hyper-local message is likely to be not relevant and disruptive to most of the audience in a large area resulting in public tune-out of all emergency messages.

Now the good news. Modern digital systems generally use more intelligent, smart devices which offer more personalization of the user experience. It’s no longer a three national TV network world which all interrupted programming to cover Presidential speeches. Smart devices can monitor emergency signals in the background and only interrupt the user based on the user’s preferences, instead of the broadcaster’s preferences. If the alert is not of interest to the user, on a smart device a user can immediately dismiss the alert, such as on mobile telephones with Wireless Emergency Alerting; instead of being forced to wait for the entire EAS message to play on traditional EAS distribution systems. On voice mail systems, users can skip messages; but advertisers want to force the public to listen to their messages and disable fast-forward and skip on DVRs.

Smart devices are usually considered consumer electronic devices, which the distribution service may or may not control directly. Digital TV broadcasters usually don’t control which digital TV’s or converter boxes consumers buy. Cable systems usually the control set-top boxes used by subscribers, but clear QAM tuners or unencrypted cable are not controlled by cable systems.

5.2. Cable Force Tuning and Selective Override

Because participation in Local EAS Area and State EAS plans is voluntary, different EAS participants frequently choose to carry different emergency messages, and which may be of importance (or irrelevant) to different parts of the audience. Various interest groups have been bickering over cable force tuning and selective override almost since the beginning of EAS in the 1990’s. Now that all types of EAS Participants operate multi-channel systems, including broadcast HD Radio and Digital TV, the force tuning and override issues are no longer limited to only cable TV systems.

In Canada, the Canadian Radio-television and Telecommunications Commission received comments as part of its public record which sometimes took opposite positions than the US industry counter-parts. Canadian Broadcasting Corporation's position was over-the-air television stations do not need to participate in (and therefore don't need to spend their money on) the Canadian National Alert Aggregation and Dissemination (NAAD) System because only 6% of viewers watched television over-the-air, and 94% of viewers would learn of any alerts and emergencies when cable and satellite distribution systems implement NPAS (and implied only cable & satellite distributors should pay to implement).[2]

I don't claim to have a complete solution, but I would like to make a few suggestions to improve the user experience from the point of view of the public, although it may create some extra burdens for broadcaster, cable and local government interest groups.

1. How important is the Presidential message to the public?
2. Improving the user experience during normal conditions and emergencies
3. Choices based on the burden on the entity that has to spend the money or pay the fines
4. Differences based on technology, not regulatory license category

There are significant differences for analog and digital systems, and 30+ years of different approaches even within analog or digital systems. Inserting EAS in a single audio channel at a radio station is very simple compared to an engineering an alert system for a multi-channel, multi-technology audio/video distribution system. Requiring channel by channel, or even sub-channel by sub-channel differences increases the complexity and burden at the head-end. The wide variation in receivers on consumer-side, and multiple generations of technology in every system, means no simple changes exist.

The traditional ways to support the EAS on analog and digital cable systems include the following:

Analog Systems in rough order of complexity expense:

- Comb generators (lowest cost)
- IF switching
- Baseband switching
- Video crawl overlays and audio replacement (highest cost)

Digital Systems in rough order of complexity/expense:

- Legacy digital set-top (vendor 1/proprietary) – Simple out-of-band signal from head-end to digital set-top boxes force tune to a designated channel.

[2] http://www.crtc.gc.ca/eng/archive/2014/2014-444.htm

- Legacy digital set-top (vendor 2/proprietary) – Out-of-band signal with commands, alert text and optional audio file.
- Set-top/Cable Card using SCTE 18 (Society of Cable Telecommunications Engineers, 2013) - Out-of-band signal with command and alert text and optional audio sources. Set-top box creates video overlay crawl from the alert text and plays the optional audio file. Cable Cards usually cannot process out-of-band audio files, and must tune to a details channel for audio. In almost all cases, Presidential alerts require force tuning to a details channel for indefinite length messages. SCTE 18 has numerous options for processing alerts, and different devices behave (and misbehave) differently.
- Clear QAM cable tuners – Because QAM tuners are not required to respond to system commands, requires EAS/PSIP override at the ASI splicer or QAM modulator at the system head-ends.

Other Systems:

- ATSC tuners – Existing ATSC tuners and converter boxes are not required to respond to digital EAS (M-EAS), requires digital splicer or PSIP override at the broadcast source. The ATSC 3.0 working groups are including EAS features in the new standard, but no assurance consumer electronic devices will implement them.
- MVPD Internet Protocol (IP) video systems – These are not Over-the-Top video systems using the public Internet, they are managed IP video providers. MVPD’s using IP video encoding have created a wide variety of methods to insert and switch programming in their systems. Because IP video systems don’t require a “head-end,” IP encoding may be performed in multiple locations, and do not have a single head-end for an EAS box.
- IPTV set-top box standardization – ATIS-0800010, Emergency Alert System Provisioning Specification. These standards specify more extensive IPTV set-top box behavior with additional alerting features during non-TV activities.
- DBS and SDARS – Due to the small number of companies, they have proprietary or unique systems.

Since the Digital TV transition in 2009 even the traditional ways analog and digital cable implemented the EAS have needed to change. Although more cable systems have switched to digital distribution, there are still thousands of analog cable systems. Analog cable systems have needed to down-convert over-the-air Digital TV 8VSB signals to analog NTSC signals for traditional analog cable subscribers. Digital cable systems can translate digital 8VSB signals to digital QAM signals, but need to up-convert analog Class-A/Low-Power TV station signals to digital QAM signals. Hybrid analog/digital cable systems (also known as dual-carriage systems) may need to do both. The digital transitions in both broadcast and cable means more systems must do more things to channels, instead of a simple antenna and amplifier, a digital analog processor may be needed. Altogether, the technological changes make it almost a case-by-case analysis of who can reasonably do what. That analysis may change year-to-year, as different systems implement changes.

5.2.1. How important is the Presidential message to the public?

While the FCC is charged by Executive Order and policy to manage the Emergency Alert System for the purpose of distributing a Presidential message, understanding that message's requirements impact on engineering choices is important. The combination of Presidential message requirements drives several of the engineering problem areas, such as force tuning and device lockups. In particular, its unique requirements to a) immediately interrupt all programming, b) carry the message "live," c) for an indefinite period of time.

In a three national TV network world, when the President made a national speech, there was almost nothing else on TV. But now in a multi-hundred channel world, there is always something else on while the President addresses the nation. Even during 9/11, when more channels than normal carried the President's speech, the Cartoon Network deliberately decided to continue running children's programs as an alternative. Is the purpose of EAS is to inform the public that the President is speaking, and inform them which channel is carrying the speech? Or is the purpose of EAS to interrupt and block all other programming on all channels and only carry the President's speech "live" for however long it lasts?

The answer to those questions dramatically affects the engineering choices, and the public's experience during an actual emergency and as well as during accidental activations. During an extreme emergency, they public will probably be actively searching for information. During an accidental activation, the public probably just wants to get back to whatever they were doing. In a decentralized, multi-channel system, forced tuning at the end-user's device may be the only way to interrupt all programming for an indefinite time. If users must tune to a different channel themselves, they may miss the emergency information.

Forced-tuning is a complex engineering challenge, which engineers felt necessary to implement to meet all the constraints of Presidential messages. When I was working on EAS for IPTV, forced-tuning was one of the most complicated parts of the system. Engineers like hard problems, but are also lazy. If we don't have to do a lot of extra engineering work, we try not to create more work for ourselves. In particular, the word "live" for Presidential messages implies any type of system delay is unacceptable, and the EAS system must be able to switch between multiple "live" sources of the Presidential message. Normal EAS messages can be buffered and streamed through digital systems with a brief delay, and don't need to switch to different sources in case of a problem. This may not have been a concern in 1994 with traditional analog broadcasters and networks.

If the FCC wants to eliminate forced-tuning as an engineering option on multi-channel systems, FEMA and the White House may also need to update or re-interpret the requirements for Presidential messages.

5.2.2. Improving the user experience during normal conditions and emergencies

Although the FCC askes about cable force tuning and selective override from the perspective of broadcaster and cable systems, there is also the perspective of user choice and user selective control of emergency alerts.

The Emergency Alert System, and the Emergency Broadcast System before it, are based on the broadcaster “push” model of distributing information to the public. The broadcaster decides when and what information the public receives, and the public has limited choice. In a “pull” model of distribution, the public decides what information they want and when they want it. In an analog, narrowband system; the push model may make practical sense. In a digital, broadband system, a pull or on-demand model may make engineering sense.

Digital TV broadcasters are now mini multi-channel video distributors. If DTV broadcasters included emergency information in the digital data stream, smart TV’s could improve the user experience filtering emergency messages of interest to the user, integrating the messages on the screen with other on-screen information such as program guides, closed captioning, and non-broadcast video sources.

This depends on the “intelligence” built-into consumer electronic equipment. Smart devices aren’t always that smart. Set-top boxes lockup. Its likely smart TV’s would also lockup. Deciding who is responsible for smart devices will have a dramatic impact on the user’s experience. During the Digital TV conversion, the NTIA required all DTV converter boxes eligible for coupons to be able to decode digital Emergency Alert System (EAS) messages. However, the FCC never required DTV stations to transmit digital EAS messages, so consumers have never been able to use that functionality in their DTV receivers and smart TVs.

The same is true for Digital Cable, Digital Satellite and Digital wireline and wireless providers. But, it is not true for analog systems. Analog systems generally use “dumb” receivers (i.e. radios and TVs), which are not programmable in the modern sense, i.e. beyond setting a timer on a VCR to record a program.

5.2.3. Choices based on the burden on the entity that has to spend the money or pay the fines

It may be possible to group analog channels, such as the FCC does with spectrum allocations. But it’s difficult to selectively group channel by channel in analog systems, especially if those decisions must allow other parties to arbitrarily switch their choices.

Broadcasters may want the use of specific analog cable channel numbers for their programming, but that makes it difficult to pack analog channels together in a coherent manner. Assuming an analog cable system was able to group all the broadcast channels together and selectively exempt channels 2-13 in their line-up. But channel 7 decides not to sign a written agreement, or channel 6 is a satellite home shopping channel, it may not be commercially practical make such fine-grained engineering changes in an analog system. In hybrid systems, with both analog and digital distribution, a consistent user experience is difficult unless you adopt a lowest-common denominator approach. While it may be possible to selectively exempt a single channel in the digital portion of the system, it may not be practical to exempt the same channel in the analog portion of the system. The EAS has generally adopted a lowest-common denominator approach with a lowest-common denominator user experience.

As a practical matter, requiring written agreements has not worked for both engineering reasons and business issues. The various parties often view those written agreements as yet another opportunity to fight with each other over a wide range of commercial practices, and looking for ways to leverage concessions from each other. So even if it may be possible for engineering reasons, its often not possible for business reasons.

> "May elect not to interrupt EAS messages from broadcast stations based upon a written agreement between all concerned. Further, analog cable systems, digital cable systems, and wireless cable systems may elect not to interrupt the programming of a broadcast station carrying news or weather related emergency information with state and local EAS messages based on a written agreement between all parties."

Changing legacy systems is always expensive. The businesses most likely to be impacted are systems which aren't able to afford to upgrade. Otherwise, they would have already spent the money for modern systems. The Digital TV transition had the advantage of billions of dollars from auctioning spectrum to pay for new digital TV converter boxes. There are still some analog TV stations. But the Digital TV transition also relied on most consumers with older TVs are connected to analog cable systems, and didn't need to pay for those transition costs. Forcing analog cable systems to switch to digital systems to support selective overrides would make the Digital TV transition costs look small.

Any risk adverse organization will naturally make a very conservative interpretation of any FCC rule. The broadcast station has no regulatory risk from a cable system's implementation of EAS. However, a cable system may decide not to risk an FCC enforcement action even with a written agreement when re-broadcasting a TV station with a defective EAS implementation. Instead their lawyers may have a belt-and-suspenders approach, and ensure its clients transmit all required EAS tests and alerts on all channels regardless of promises from some other party. Historically, the FCC enforcement has decided a licensee can't shift responsibility just because it has a written agreement.

5.2.4. Differences based on technology, not regulatory license category

I would like to suggest the FCC adopt some more general principles instead of per-license category rules. The EAS rules attempted to finesse (i.e. punt the can down the road) the issue of selective overrides with slightly different rules for cable, satellite video, satellite audio, radio translators, TV boosters, FM antenna service via cable, etc. Actually there aren't any EAS rules for FM antenna service via cable or carrier current campus radio stations. The FCC could indicate the goal is avoiding overlapping EAS notifications in the same programming, but the trade-off between missing important local alerts on some channels versus duplicate irrelevant alerts on some channels will still occur.

My suggested guidelines or principles include:

1. EAS Participants are **not required** to interrupt programming channels which entirely rebroadcast the programming of another EAS Participant from the same local EAS area, and passes through EAS activations and tests.

    Local-into-local programming from other EAS participants already includes local EAS alerts. No written agreement is needed, because FCC rules already require those programming sources implement a compliant EAS system. Its only liable for its own actions, i.e. it must pass through EAS messages which they generally do anyway, and clearer the EAS participant should not be liable for the other EAS participants. This applies to FM translators, HD radio sub-channels carrying programming from another local radio station, satellite TV systems, as well as cable TV systems carrying "local-into-local" channels.

    This would allow analog systems to group all local channels together with a simple filter or combiner, without needing to engineer exceptions depending on individual local channels deciding to sign or revoking written agreements. However, the "not required" would still allow a system to interrupt local channels for engineering (i.e. some analog systems can't practically re-engineer systems or a broadcaster demands a specific analog channel number beyond those covered by a filter) or a university campus or military base uses the system as part of its local mass notification systems. The "local EAS area" constraint is important because some satellite-feed programming may be from an EAS participant in a distant area which doesn't contain local EAS alerts.

2. EAS Participants using digital service multiplex and transport systems must also transmit emergency information as part of the ancillary digital data streams to enable smart devices to filter emergency alerts based on the consumer's choices. They should continue to distribute EAS alerts on at least one channel if a key EAS monitoring source.

    Another challenge will be coming up with a term for smart digital systems which doesn't become technologically obsolete. The term "digital service multiplex and transport system" is based on MPEG-TS technology, but shouldn't be limited to only ATSC and DVB. IPTV systems are functionally equivalent multiplexed services although they are packet based instead of transport stream based. Some digital technologies such as ATSC haven't standardized EAS via a digital data stream yet, but are working on it.

    Unless EAS Participants begin to distribute emergency information through digital data streams, it will be difficult for smart devices to implement user-controlled alert filters. User-controlled choice was part of the original EAS

> *Implementation order, but had limited success beyond weather radios. This applies not only to "Open Set Top" initiatives, but Digital TV broadcasters for Smart TVs and Digital Audio broadcasters for Smart Radios.*
>
> *Satellite distributors currently do not distribute local EAS alerts, other than local-in-local pass through, because it doesn't make sense to interrupt national programming for a local alert. Distributing emergency information through the digital data stream would enable regional groups of satellite receives to implement local emergency alerts, much like local sports blackouts.*

3. EAS Participants which sell or lease smart devices to consumers must ensure those devices can selectively exempt channels which pass through EAS activations and tests as part of their programming.

> *The FCC should also encourage other consumer electronic devices bought directly by consumers from other sources, such as smart TVs and smart radios, support selective exemption and improved user filtering of emergency alerts. The FCC has already done this with mobile telephones and Wireless Emergency Alerting. Responsibility for ensuring smart devices work with the EAS system will be problematic, because the consumer electronic marketplace tends to change much faster. Consumer electronic manufactures are good at implementing standards, assuming consumer electronic standards are created.*
>
> *As smart devices get smarter, it is likely they will be able to integrate emergency information from multiple sources on the same screen. The FCC should not prohibit better integration of set-top boxes, electronic program guides, picture-in-picture, coordinating close captioning and emergency information crawls, and so on. Broadcasters should not have an exclusive claim to the video real-estate on the user's television screen. Selectively exempting a channel for EAS should mean exempting the channel from "forced-tuning" but still permitting on-screen program guide alerting.*

4. EAS Participants may elect not to interrupt programming sources carrying news or weather related emergency information from other voluntary EAS participants, e.g. NY1 in New York City, with written agreement that the programming provider implements its own compliant EAS system and participates in the same local EAS area plan.

> *A written agreement is required in this case because of the voluntary nature of the compliance of non-FCC licensed programming sources. If the voluntary EAS programming source violates FCC rules for EAS, the EAS Participant should be responsible for terminating the voluntary EAS agreement. If the EAS Participant will still be subject to fines for violations under the written agreement, they will probably these types of agreements.*

> *Again, this should not be limited to cable TV systems. Satellite-fed radio and TV broadcast sub-channels could also do this. Some local Public, Educational, Government (PEG) channels may want to take advantage of this for emergency information in their local franchise area.*

5.3. EAS on Programmed Channels

EAS should be focused on mass media programming channels. EAS should not be considered the only public warning system, or the only tool in the warning toolbox. EAS should be considered as a complementary part of an overall public alerting system.

In a "push" broadcast model of programming, any alert is usually considered a disruptive interruption. Although a temporary distraction can become annoying interruptions, such as Twitter "tweet storm" which turns a pull into a push. A difference is users expect more control over on-demand activities compared to broadcast programming. Even the term "programmed channel" reflects the push approach. Users perceive different activities, even on the same system, in different terms than "channels." It's a multi-tasking, on-demand world with multiple-screens and multiple-applications being used at the same time.

In analog narrowband channels, interrupting the programming channel was often the only choice. With broadband communications, there are more ways to notify the audience of emergency information.

When I worked on engineering EAS over IPTV, I made a choice that EAS messages were not associated with a "channel." By not associating EAS alerts with channels, individual IPTV subscribers could have more control over when and what types of alerts pop-up on their screens. They could independently dismiss EAS alerts without waiting for the entire audio message to play, except for Presidential "live" messages. By not inserting the EAS message into the program stream, a subscriber could retrieve the EAS message later instead of one-shot and its gone. And subscribers did not have out-of-date EAS message in their DVR recordings because the EAS message wasn't part of the recorded video stream. Except for Presidential "live" messages stream due to its indefinite length requirement.

Nevertheless, maintaining the illusion and behavior of "program channels" can be important for user expectations, even if the technology doesn't require it. Forcing viewers to tune to a different channel or click to get an emergency alert during a radio or TV show can be unexpected behavior for most people. The principle of least user astonishment may be to play the EAS message automatically on TV-like services. An IPTV system may be configured to avoid interrupting the user while watching local broadcast TV channels and only include an "alert-active" graphic in the on-screen program guide. While user is watching a satellite-feed channel, the IPTV set-top could insert the full EAS experience and automatically interrupt the program with an on-screen video overlay and play the EAS audio. But when the user is watching a pay-per-view "live" event, the IPTV set-top may only interrupt the user for extreme threat EAS messages. The user could change their set-top box configuration to ignore distant alerts and tests. In theory, set-top boxes could alert users even when it is in a stand-by state. However, most people are unpleasantly upset when a device they think is “off,” and it does something. So most consumer electronic devices avoid any user visible activity while in a stand-by state.

Because Internet and other data channels are used for computer communications, software gets very confused and may crash when data channels are interrupted. Broadband channels used for Internet/data shouldn’t be considered mass-media channels for EAS rules. Instead, an application on those computers could “pull” emergency information and pop-up an alert on the computer screen. In the 1990’s, several ISPs experimented with caller-id applications which would pop-up an alert with a caller’s telephone number while the user was using a dial-up modem. It wasn’t very popular with users. If an Internet or computer public alerting application is developed, it should be treated as a different public alerting system from the EAS.

The public does not expect in-progress telephone calls to be interrupted by the EAS or WEA. When a telephone operator makes an emergency “barge in,” or busy line interrupt, it tends to surprise the callers. Broadband channels used for telephony should not be considered mass-media channels for EAS rules. Other public alerting systems using telephony, such a mass-calling systems have different processes and issues, and should be handled under telephony rules.

And finally, EAS has always ignored other non-video cable channels such as audio-only cable music channels and FM antenna service over coaxial cable service.

5.4. EAS Alerting and Emerging Video Technology

Different alerting systems should not attempt to emulate exactly how other alert systems work, because sometimes those alert system features are really annoying “bugs.”

Wireless Emergency Alerting doesn’t attempt to interrupt the voice channel on a mobile phone. People would find that behavior very annoying and disruptive. Instead, WEA uses data control channels to alert the public through the phone’s message capability.

IPAWS and the Common Alerting Protocol is open to new computer applications. Google Crisis Response team created an experimental public alert application.[3] Public Alerts are integrated into Google Search. If you search for a place where there is an alert active, or from within an affected area, you’ll see a warning, and can click through to find out more information.

A common challenge for any emerging technology is gaining access to existing sources of information. While Google has enough market power to gain access to most public information, often traditional market players consider existing systems and information to be their property. They may claim the need to limit access for reasons of security, intellectual property, public confusion, etc. FCC should continue to emphasize government warning information is public information, and use of the EAS automatically grants rebroadcast

[3] http://google.org/publicalerts

authority and use by the public as well as new emerging technology market entrants. Federal, state and local CAP aggregation systems should be open to emerging technology and companies. The content of CAP messages is in the public domain, or automatically grants public license to use the CAP messages.

5.5. Technological Potential for Improvements in Accessibility

FCC should distinguish between presenting warning information in more accurate and accessible ways; and changing the warning information through translation or interpretation.

Some EAS participants have graciously volunteered to translate warning information in their local areas, e.g. local primary stations for Spanish, Korean and a few other languages. However, it is always difficult to get all the nuances correct in a translation without being able to check what the original authors intent was. At official events, sign language and foreign language interpreters often receive advance copies or background information in preparation. Machine translation continues to improve, but even machine translation makes mistakes or needs to check its translation with the original author. That can't happen after an EAS message is transmitted, and unreasonable to expect every EAS Participant to do something a government agency was unwilling to do itself.

Government originators should continue to work with volunteer EAS participants translating warning information before the EAS message is released. There are communication channels which could be used to coordinate between language volunteers and governmental agencies outside of the EAS. Even during disasters, language volunteers and governmental staff are usually able to reach each other. Local emergency agencies in areas with significant non-English speaking populations usually already include language assistance in their government emergency plans and have people on staff able to speak other languages. Only the government alert originator can determine when the delay contacting language volunteers for assistance is acceptable versus immediately releasing a single language alert and following up with other language populations. EAS should never be considered the only way or the only information to reach the public. The EAS is always part of an overall public alerting and information dissemination process. News broadcasts and reporters at EAS Participants will continue to cover an emergency after the initial EAS alert message.

Once the governmental originator, with the potential assistance of language volunteers, prepares the multi-lingual messages, CAP can transport the messages in multiple languages. When the CAP information is released, other EAS participants should not be expected to change the content of the warning information. Downstream EAS participants do not know the context and would not be able to double check their interpretation of the alert information.

Improving the presentation and accessibility of the warning information is a different issue. Older EAS systems and video character generators used only ASCII characters and low-bandwidth audio. Broadcast announcers sometimes re-record emergency messages with a "professional announcer voice," but should not change the content of the emergency message. Characters with diacritical marks or non-Latin script were often mangled or just not displayed on video crawls. Some county names in territories include diacritical marks, which the public may have gotten used to missing, but it is still insensitive. The Common Alerting Protocol supports Unicode UTF-8 encoding allowing world-wide languages. It may be unreasonable to expect EAS participants to be able to present every world-wide language, but participants are usually able to support the language(s) of their primary audience.

To the extent possible, video programming EAS participants should present readable text of alerts, as prepared by the alert originator, using the proper character glyphs in the languages of their primary audiences. Although the definition of readable text messages and understandable voice messages are always debatable, as evidenced by the small print and fast speech in used car ads; the reasonable person test generally works with occasional enforcement reminders.

Digital EAS participants (audio and video) should also transmit the alert data or warning codes as part of the digital ancillary data stream for display or use by smart receivers. The consumer electronics industry may use the digital ancillary data stream for other accessibility capabilities. This will be an integration and interoperability problem for industry to work on a solution. Fortunately, most of the technical work is already being done to support advertising and shopping, so the EAS may be able to leverage many of the same capabilities.

6. Securing the EAS

In addition to unauthorized EAS alerts, analysis of EAS security should include the impact of missed alerts and operational complexity risks. A simplistic way to avoid the risk of a false alert is never relay any alerts. Better EAS protocol technical specification and more detailed EAS Operating Handbook would enable automated EAS devices and EAS participants to better validate EAS messages. EAS equipment is more similar to an industrial control system than a general purpose computer server. NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security (National Institute of Standards and Technology, 2015) contains many concepts applicable to EAS operational systems.

6.1. Essential Factors from the Former Emergency Broadcast System

The Office of Telecommunications Policy, Emergency Broadcast System Procedures Manual (Office of Telecommunications Policy, 1974) described the EBS as:

> “The national Emergency Broadcast System (EBS) provides the President and Federal Government authorities a ***readily available, reliable, and low-cost*** means of emergency communication with the American people. It backs up the normal means of arranging a nationwide broadcast through the radio and television networks and affords a capability in grave emergencies when national communications resources have been disrupted. National EBS broadcasts may be used to reassure and give direction to the American people regarding survival and recovery of the nation.” (emphasis added)

More specifically, in Annex J: Emergency Broadcast System Briefing in the Aerospace Defense Command’s EBS Procedures (Areospace Defense Command, 1976), four essential factors were identified:

> “Background - Several factors were considered essential in establishing an EBS to back-up the normal means of arranging a nationwide broadcast for the President.
> (1) The system should have ***adequate control measures to preclude inadvertent activation*** of the system, and it should be ***reliable, readily available, and generally low in cost***.
> (2) To further clarify these four terms, define in the context of EBS.
>
> > (a) As you may recall, in Feb 71, an actual activation message was released in lieu of a test message by the NWC who at that time was the primary control point. To insure that a similar instance would not occur, additional controls were to be established throughout the release of an EBS message with several safeguards incorporated in the EBS TTY tape messages. More details concerning these measures will be covered later in the briefing.
> > (b) By reliability, it was recommended that more than one release point for activation and numerous recipients of this information be included in the system. So if a certain portion of the notification network was inoperative, the system could still be activated.

> (c) By availability, it was meant that existing facilities should be used where possible.
> {d) By low in cost, in addition to using existing facilities, it was suggested that industry share a burden of the cost." (emphasis added)

Assuming the same four essential factors from EBS also apply to the Emergency Alert System, these factors can serve as the basis for evaluating security proposals for EAS. Since the current White House Statement of Requirements has not been publically published, the actual factors are not available for evaluation.

6.2. Risks in EAS Protocol and Operating Specifications

In order for a EAS device and participant to verify and validate an EAS message, they need to know what a valid message should be. Ambiguities and inconsistencies in the protocol specification and lack of published current operating procedures contribute to security problems.

A general principle of robustness for technical protocols is "be conservative in what you do; be liberal in what you accept from others." While robustness is a good general rule of thumb for technical protocols, it also affects the security of a system. The Internet Engineering Task Force documented and expanded the robustness principle in RFC1122, "Requirements for Internet Hosts -- Communication Layers." (Internet Engineering Task Force, 1989)

> ### Robustness Principle
>
> At every layer of the protocols, there is a general rule whose application can lead to enormous benefits in robustness and interoperability [IP:1]: "Be liberal in what you accept, and conservative in what you send"
>
> Software should be written to deal with every conceivable error, no matter how unlikely; sooner or later a packet will come in with that particular combination of errors and attributes, and unless the software is prepared, chaos can ensue. In general, it is best to assume that the network is filled with malevolent entities that will send in packets designed to have the worst possible effect. This assumption will lead to suitable protective design, although the most serious problems in the Internet have been caused by unenvisaged mechanisms triggered by low-probability events; mere human malice would never have taken so devious a course!
>
> Adaptability to change must be designed into all levels of Internet host software. As a simple example, consider a protocol specification that contains an enumeration of values for a particular header field -- e.g., a type field, a port number, or an error code; this enumeration must be assumed to be incomplete. Thus, if a protocol specification defines four possible error codes, the software must not break when a fifth code shows up. An undefined code might be logged (see below), but it must not cause a failure.
>
> The second part of the principle is almost as important: software on other hosts may contain deficiencies that make it unwise to exploit legal but obscure protocol features.

> It is unwise to stray far from the obvious and simple, lest untoward effects result elsewhere. A corollary of this is "watch out for misbehaving hosts"; host software should be prepared, not just to survive other misbehaving hosts, but also to cooperate to limit the amount of disruption such hosts can cause to the shared communication facility.

Many of the IETF principles in RFC1122 are also applicable to non-Internet protocols, such as the EAS Protocol and the Common Alerting Protocol (CAP). But there is a limit to how far you can stretch the robustness principle. Technical standards organizations often publish corrections and clarifications as different implementers identify different ways of interpreting a technical standard. Just because an implementation made a choice that worked in a particular situation, while other implementations made a choice that didn't work, does not absolve an ambiguity in the specification of contributing the problem. After analysis, often there are cases where the first implementation may not work in a different situation, while the other implementations would work. That doesn't not mean any particular interpretation was "wrong," but for interoperability they must reach an agreement on a common interpretation.

Simply blaming old equipment or operator error is often a cursory analysis of problems. The incomplete or ambiguous specification for the EAS protocol and inconsistent information in sources like the EAS Operating Handbook are also contributing factors. Brittle systems tend to break when exposed to stress. If the system requires extraordinary operator abilities and omniscient equipment, it may not be suitable for use during extremely stressful situations such as a catastrophe.

6.3. Improving EAS Protocol Specifications and Operating Handbooks

By necessity, regulations are written to be open ended so an agency can make judgements of good faith and resolve unforeseen problems later. Regulations aren't expected to be as detailed as technical specifications. However, for automated, unattended systems, open ended technical language often leads to unexpected and insecure results. Writing the EAS Protocol technical specifications in regulatory language has created ambiguities and engineering problems.

In 1994, the FCC relied on security by obscurity choosing non-standard modem tones, instead of the common Bell 202 (300 baud) or Bell 212 (1200 baud) modem standards, assuming most people would not have access to equipment which could generate EAS data bursts. Other than the obscurity of the protocol itself, there are essentially no built-in protocol security features. In 1994, programmable digital signal processing (DSP) chips were relatively expensive.

> "The EAS code protocol uses a non-standard data rate and shift frequencies. The reason for use of non-standard digital signaling is to allow it to be claimed as an exclusive government emergency warning standard and thus control its use. Non-standard signaling should not increase the complexity of the equipment or components, but does mean that hardware must be designed specifically for this purpose. Thus, off-the-shelf devices cannot be used directly, making it more difficult for intruders to break into the system." (footnote 88, EAS deployment order, 1994 R&O and FNPRM)

Now CPUs in personal computers, smart phones, tablets, etc. are powerful enough to easily generate high quality EAS tones and AFSK data bursts without needing an external DSP. The Silicon Labs SI4707 chip including Specific Area Message Encoding (SAME) is approximately $18 (single unit quantity, March 15, 2015). Hobbyist kits are approximately $30-$60 for EAS/SAME protocol decoders, and $70-$100 for EAS/SAME protocol encoders. Consumer quality digital recording technology can make copies indistinguishable from the original.

Throughout these comments, I suggest several incremental improvements and clarifications to the SAME/EAS protocol which would help reduce accidental EAS incidents, not deliberate targeted attacks. Interoperability between different vendors acts as a limit to how well it can be secured without a complete re-design of the SAME/EAS protocol. While each EAS vendor’s equipment is compatible with itself, there are often subtle differences in interpretations between vendors which are only found through extensive interoperability testing and field experience. More radical changes, such as strong digital signatures, would break compatibility with existing EAS and weather radio decoders, or would be too complex and costly to justify replacing current EAS equipment. Ultimately, the FCC is faced with the same choice for the EAS, as AT&T had to make in the 1960’s for the public switched telephone network. AT&T needed to change in-band signaling, like the 2600 Hz toll tone, to an out-of-band signaling system (SS7). In the 1980’s, radio and television networks used in-band cue tones. Since then most broadcast networks have changed to out-of-band or digital cue signaling.

Updating the FCC EAS Operating Handbook may be a way to distribute more detailed, technical information that wasn’t included in the EAS regulations. But relying only on the handbook and an operator is less viable with unattended, automated systems. Instead, better technical specifications are needed for automated systems. The Wireless Emergency Alert system uses the Alliance for Telecommunications Industry Solutions (ATIS) as the maintenance agency for CMAS standards instead of writing them in WEA regulations. FCC should consider delegating the technical maintenance of EAS Protocol standards to a professional standards organization.

The FCC does not directly regulate state, local and other government agencies; but in coordination with FEMA, FCC can work with governmental sources of emergency information. FEMA currently provides training and certification for government agencies using IPAWS. The FCC EAS Operating Handbook should be updated with information how the EAS system now works, how EAS originators (including other government agencies) should prepare messages and how EAS participants (and their automated systems) should validate messages. In addition, FEMA should work with its constituencies on chapters and manuals to include in their emergency management and communication plans.

6.4. Improving EAS Equipment Certification

EAS participants are dependent on the security functions built into their EAS devices. It is extremely difficult to add security later to an insecure system. EAS equipment manufactures play a critical role in the overall security of the EAS ecosystem. The default configuration settings in equipment act as the first, and often most powerful security policy for the system.

Automobile manufacturers used to always blame drivers for being killed in car crashes. Automobile safety engineering now recognizes the role of the car design in its safety. Likewise, the security of computers is often dependent in the security design of the system. Making operators or users solely responsible for security afterwards is unrealistic.

As part of the certification of acceptable readiness of the EAS equipment, EAS manufacturers should test the security mechanisms to verify they work as claimed in the manufacturer's system documentation and EAS regulations and Operating Handbook. Independent testing should also be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security mechanisms in the initial out-of-the-box configuration based on the manufacturer's written security guidance. This is commonly called penetration testing or red teaming.

EAS manufacturers should also include a single summary, chapter or manual in the user documentation describing the security mechanisms provided, guidelines on their use, and how they interact with one another. Installation instructions should provide security guidance for the initial out-of-the-box configuration and security cautions. The manufacturer's guidance may be based on a basic and simplistic security policy for common network architectures. The EAS Participant is responsible for developing specific security policies that meets their needs, but the EAS manufacturer knows their particular products best. Although this may seem obvious, the "Orange Book" (National Computer Security Center, 1983) included the requirement in 1983, experience has shown the need.

Ongoing software maintenance and software warranties are extremely complex commercial and legal problems. If a system cannot be patched or updated, software security problems identified later can't be fixed. Software maintenance also increases the manufacturer's costs, which will be passed along to customers. While hardware may be fixed by anyone with the appropriate technical ability, embedded system software often can only be fixed by the manufacturer. If a manufacturer goes out of business, there may be no further software support for its products. These risks exist for all software products. The risk for the EAS system is other EAS Participants depend on each other the proper functioning of those EAS devices.

6.5. Improving EAS Network Security

6.5.1. Annual Certification

A challenge for information security is a constantly evolving adversary. Best practices need to continually improve. Any static list of requirements will quickly become outdated, but the basics tend to remain the same. Other federal regulatory agencies have tried different approaches. The Federal Financial Institutions Examination Council has extensive handbooks used by its regulatory members the FCC may want to review.

EAS Participants already have an obligation to comply with all FCC rules and regulations. A special certification process for a few information security items may distract management from their overall EAS operational responsibilities. Including a general security responsibility for EAS participants in § 11.35 Equipment operational readiness may be an alternative approach.

The FCC Media Bureau maintains Broadcast Self-Inspection Checklists, including a section on the Emergency Alert System.[4] The checklists could be updated with EAS Participant security responsibilities. Several industry associations manage independent self-inspection programs. An independent security assessment is preferable to self-certification, as long as the independent assessor is qualified technically. This is widely done in the financial industry, such as the Payment Card Industry (PCI) compliance programs.

Identifying only a few security responsibilities is always difficult, because management will always view "minimum" requirements as the "maximum" required. But if the FCC does list a few basic security responsibilities for EAS Participants, I suggest the following:

- Protect against unauthorized access
- Defense in depth
- Remediate identified vulnerabilities
- Incident response plan
- CAP digital signature validation

6.5.2. False Alert Reporting

Most of the time it is obvious an alert is false. Sometimes it takes a long time to verify if an alert is real or false. In 1971, it took over 40 minutes to issue a valid EBS cancellation message after the National Emergency Warning Center accidently transmitted a "real" alert message instead of the scheduled test message. FCC and its government partners need to decide and publically say whether the objective is absolute certainty an alert is valid, or immediacy is better than delay. In the news business, editors know that scooping the competition is important, but accuracy is just as important to their credibility.

As the FCC is aware, the Network Outage Report System (NORS) is limited to significant, major outages and critical infrastructure, not every outage. That greatly reduces the reporting burden on NORS participants and the FCC. Generally, NORS only requires the responsible communications provider to submit a notification within 120 minutes, initial report within 72 hours and a final report within 30 days; with some differences for different types of providers. Generally, only the responsible communications provider must file a report, not any other communication providers which depended on the provider.

[4] https://www.fcc.gov/general/broadcast-self-inspection-checklists

As much as possible, false, corrupted and other EAS operational problems should be handled quickly at the lowest operational level. Reports may be completed later, after management and legal reviews. I suggest the FCC consider different thresholds and notification procedures.

1. EAS participants and EAS originators should quickly notify other EAS participants within their state/local area which may have been impacted by a simulated, false, corrupted or other operational problem with EAS transmissions for immediate corrective action. Often an originator doesn't realize they caused a problem until other EAS participants inform them. Most states and some local EAS areas maintain email lists, phone trees, and know each other. This may be done informally between EAS participant and EAS originators, i.e. engineer to engineer, whether or not FCC/FEMA needs to be notified.
2. In the event of a simulated, false or corrupt EAS alerts which impact a large number of people; or any false or simulated EAN message, the responsible EAS participant, or first EAS participant relay if the source is unknown or not an EAS participant, should submit a quick notification to FCC/FEMA within 120 minutes. The quick notification contains only limited information, which may be incomplete or not fully verified. Because the FCC requires a person be authorized to submit information to the FCC, it may take longer to contact the appropriate authorized person.
3. The responsible EAS participant should submit a more detailed initial report to FCC within 72 hours. And a final report should be submitted within 30 days.

Please also refer to section 6.5.4 Alert Authentication for additional ways to quickly learn about false alerts.

6.5.3. Lockout Notification

All EAS system must include a manual Global Abort to reset the system to normal operation, including during an EAN message, without needing to unplug or reboot equipment. In 2006, I was evaluating EAS systems as part of a multi-state IPTV system. I included a Global Abort requirement. The EAS vendor indicated the FCC did not permit EAS systems to interrupt an EAN message while it was in progress, and would not include the Global Abort feature.

Automated, unattended EAS systems, analog and digital, will experienced system lockups until someone resets the system. Because multichannel video providers are currently the dominant media distribution system for most American households, problems with multichannel video systems are more noticeable by the public.

EAS rules were originally written in an analog, narrowband world with a single program per channel. Since then the FCC amended the rules for multichannel and digital providers inconsistently. The EAS rules still tend to have a broadcaster driven philosophy, i.e. the broadcast controls the channel, instead of a consumer (viewer, listener) driven philosophy, i.e. the public controls what they want. Wireless Emergency Alerts rules avoid some of the EAS problems by prohibiting preemption of voice and data calls. With digital distribution channels and smart devices, the consumer can have more control over what programming they get.

Smart devices can have electronic program guides, overlay multiple channels (picture-in-picture), pop up alerts from caller-id or twitter, across all “channels.”

A false alert occurs is often incomplete or partially corrupt. This leaves the EAS system and downstream participants in an indeterminate state. The EAS Operating Handbook and EAS rules should include an affirmative obligation for participants and originators to transmit an EAS reset as soon as possible when they realize a false or corrupt alert was transmitted. This may either be a simple RWT, if the EAS encoder is working; or even a recording of the End-of-Message (EOM) in AFSK, if an EAS encoder is offline or not available.

Critical EAS Participants, i.e. SP/NP stations, and large multichannel systems, i.e. more than 30,000 subscribers, using unattended, automated EAS systems should have monitoring systems to notify a responsible person when an EAS system overrides programming for more than two-and-half minutes. The responsible person should be able to verify the operation of the EAS system within 15 minutes, e.g. listen if a valid EAN message is in progress. If the EAS system is locked or not processing a valid message, the responsible person should be able to take action to reset the EAS system and downstream devices controlled by it, e.g. set-top boxes, smart TVs, etc.

To further mitigate unattended EAS systems locked by an EAN message, EAN messages should have a maximum time limit. While most downstream EAS decoders automatically reset and clear EAS messages after two minutes, EAN messages currently have no time limit. A false or corrupted EAN message may leave downstream, unattended EAS decoders in a locked state. The EAS protocol specification should be updated with a maximum time limit for EAN messages, and enable an automatic EAS decoder reset. I suggest using the +TTTT Valid Time Period as the minimum elapsed time for EAN messages. This would enable EAN messages lasting between 15 minutes and 99 hours and 30 minutes, determined by FEMA when it transmits the EAN header for a Presidential Alert. EAN messages less than +TTTT would still end with an end-of-message (EOM).

I suggest two reporting thresholds to reduce the reporting burden to significant lockout events.

1. EAS system problems which interrupt programming for 30,000 or more households for more than 30 minutes should submit a quick notification within 120 minutes, an initial report within 72 hours and a final report within 30 days.
2. EAS system problems which interrupt programming for less than 30,000 households for more than 120 minutes should be submit an initial report within 72 hours, and a final report within 30 days.

6.5.4. Alert Authentication

CAP systems should be encouraged to use digital signatures, and when implemented by the state/local CAP system, unsigned or incorrectly signed CAP messages should be rejected (and logged for review). Digital signing keys should be regularly changed, and EAS equipment will need to be regularly updated with new verification key or certificate authority information.

FEMA and/or FCC should maintain multiple secondary channels for EAS Participants to verify a national EAS activation. When a national emergency message is issued, FEMA/FCC should immediately update a national telephone recording, secondary web site and national wire services confirming a national EAS activation. A large number of access attempts on the secondary verification channels (telephone call attempts, web page hits, etc.) would also alert FEMA/FCC that something prompted EAS participants to check if a national alert was issued. EAS participants should not delay an EAN message while checking, or if the secondary confirmation channels are unreachable, or have a neutral message (neither confirming nor denying a national EAS activation). If the FEMA/FCC secondary confirmation channels verify a false alert was issued, EAS participants can take appropriate actions.

A more complex alternative is possible for EAS decoders integrated with CAP systems. They could leverage IP connectivity to check the FEMA IPAWS site asynchronously while processing an EAN message. If the IPAWS web site securely issues a CAP cancellation message for the EAN alert, the EAS decoder could automatically reset. If the IPAWS site is unreachable or does not issue a cancellation message, the EAS decoder continues processing the EAN message as normal. This provides additional national alert authentication when national networks are operational, and retains the disaster resilience of the EAS system when national networks are not operational. On really bad days, when national networks are not operational, the public is probably already looking for information and EAS Participants are probably already working on their systems. Authentication is more important for “Sunny Day” incidents, when no one expects an alert.

With complexity comes additional operational risk the system won’t work when most needed. Key management complexity is always a problem in every authentication system. Digital signatures and public key encryption are powerful authentication mechanisms, and I recommend new digital systems like CAP include digital signatures. I suggest caution trying to back fit digital signatures in legacy EAS protocols. Also recognize the limits of digital signatures. Adversaries can steal signing keys when they break into systems, and sign their own messages. Because digital signing keys can be compromised, the key management system must also handle key revocation. Re-useable authentication codes, such as the old red envelope help protect against accidental EAN activations, but not deliberate. All EAS participants and likely a large number of other emergency watchers would learn the valid codes at the same time, unless yet another system to control the distribution and control who has access to the re-useable codes would be needed.

The 1971 false EBS incident showed key management of even simple code words like “HATEFULL” and the cancellation code word “IMPISH” are difficult to manage. Key management needs to be used frequently to be robust. A system which delays the EAN message for more than a few seconds for manual review will cause problems unattended, automated EAS systems for “live” broadcasts. EAS systems usually have limited audio buffering for “live” broadcasts. EAS Participants staffed 24/7 can use human experience and respond quickly to problematic EAS messages, as has been demonstrated during past false EBS and EAS activations.

Because the Common Alerting Protocol is the only way for State/Local emergency authorities to initiate Wireless Emergency Alert messages, I expect most states and major local emergency authorities will eventually use IPAWS and state CAP systems as the primary activation method. Although legacy EAS AFSK should be retained as a disaster backup distribution system until a replacement digital over-the-air distribution is possible, only limited EAS protocol changes are realistic.

6.5.5. Alert Validation

While the FCC may write rules that require everyone and every system to always operate correctly, the robustness principle reminds us that “Software should be written to deal with every conceivable error.” Clocks won’t be correct, communication channels will be interrupted in mid-transmission, duplicate messages will be sent, configurations will be wrong, encryption will be wrong, and so on. On January 26, 2016, BBC Radio in the United Kingdom experienced nation-wide problems due to a 13 microsecond GPS satellite failure. On March 19, 2012, the U.S. Naval Observatory NTP system rebooted, and reset its clock back to the year 2000. Some local Emergency Operation Centers (EOCs) still use EAS equipment which hasn’t been updated for the 2007 Daylight Savings Time changes, and need to make manual clock adjustments twice a year.

Alert validation includes not only what is correct, but what is allowed to be wrong and what to do when its wrong. Emergency warning systems should avoid being “brittle,” i.e. failing catastrophically, due to simple errors. A Fault Tree Analysis, and another engineering process, are used in reliability engineering to understand how systems can fail, and identify the best ways to reduce risk.

Should old alerts be rejected? How long ago?

Should future alerts be rejected? How far in the future?

Should unexpected sources be rejected? How are authorized sources changed?

Which combination of EAS codes are valid for which alerts? ZCZC-PEP-EAN-000000+0015- etc. or ZCZC-PEP-CDW-000000+0100- etc. What if there is an overlap between All of Canada and All of U.S. alerts.

What if a different alert interrupts an alert? Some EAS Participants have two EAS devices installed in series, such as PEP stations and NWS Radio stations which also transmit local EAS alerts.

What if an alert never ends? Most of the time it’s an error, but an EAN may last a long time.

EAS manufactures and government testing labs should verify both correct operation, and also proper handling of incorrect conditions in a multi-vendor environment. This is sometimes called fuzzing.

Adding the year to the EAS header would improve detection of old alert recordings being replayed. It would not prevent operator error selecting the wrong event code, and transmitting an EAN event code, since it would contain the current date. If the FCC adds the year to the EAS protocol header, I suggest not inserting the YYYY in the middle of the EAS header, which will immediately break all legacy EAS and SAME equipment. I suggest adding YYYY at the end of the current EAS header. Legacy EAS and SAME decoders typically treat the inter-header 1-second gap as RF noise, so extra data characters would be ignored. FCC rules do not include any protocol transmission tolerances, but the National Weather Service SAME protocol (National Weather Service, 2011) specifies a 5% tolerance within the 1 second gap between header transmissions. 50 milliseconds allow 3.25 characters within the tolerance. With testing, it may be possible Legacy EAS and SAME decoder chips will tolerate a two-digit year YY instead of a four-digit year YYYY. But that is not the end of the compatibility issues. Relaying devices may drop the YYYY, originators which don't upgrade their systems will still send EAS/SAME messages without YYYY. Deciding on the rules for duplicate detection and preventing looping messages will be complicated. It still doesn't prevent someone or a misconfiguration from sending a EAS message with a future date, such as the year 9999, which would not expire for a very long time.

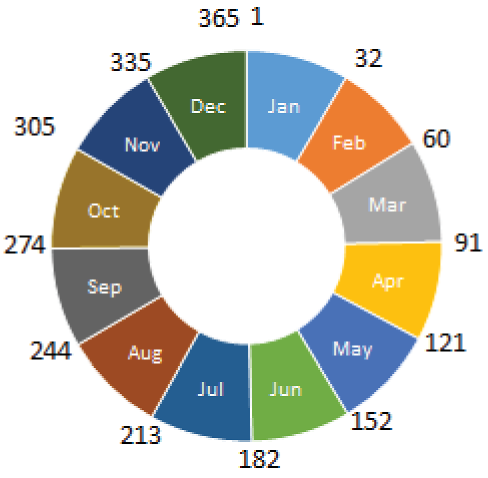


Figure 3 EAS Julian Day Calendar (JJJHHMM)

Specifying clock tolerances in the EAS specification would not require changing the transmission protocol or create incompatibilities with legacy EAS and SAME decoders. Tightening the acceptable clock skew would reduce, not eliminate, the window for message replay attacks in the EAS protocol. A small acceptable clock skew should permit both valid EAS messages when the EAS originator clock is not exactly synchronized, such as the 2011 National EAN test clock being 3 minutes fast, and accidental message replays, such as news stories which covered the EAN test and talent playing recordings on the air. It would not prevent deliberate attackers creating new EAS messages with manually set clocks or replaying an old EAS message exactly during the original clock window. The term “strict time” used by one implementer just reflects its tight or loose clock tolerance setting. It doesn’t address interoperability with other implementations. Different implementations have different clock tolerances, which means they will reject and accept different messages. Testing with at least 1 minute, 10 minute, 1 hour, 10 hour, 1 day, 10 day, 1 month, 10 month time differences should be done.

Table 4 Clock Skew Variations

		Decoder Clock		
	+0030	Slow 11:00	On-time 12:00	Fast 13:00
Encoder Clock	Slow 11:00	Not Expired	Expired	Expired
	On-time 12:00	Not Expired	Synchronized Valid	Expired
	Fast 13:00	Not Expired	Not Expired	Not Expired

Validating the ID Stamp (LLLLLLLL) would reduce the risk of EAS message replay attacks, EAS tones in commercials or other pre-recorded audio such as news stories about alerts. It would not prevent operator error accidently selecting the wrong event code or deliberate attacks generating new EAS messages. The exposure would be reduced to the same transmission source (LLLLLLLL) and downstream relays, instead of all EAS monitoring sources nationwide such as happens with embedded audio in a nationwide satellite program. The ID Stamp does not need to be unique, but should be semi-unique between EAS sources. Changes to the ID stamp would need to be coordinate with both EAS sources and monitoring participants. Out of date ID Stamps and misconfigurations would be detected during Required Weekly Test (RWT) messages. The use of PSID or FID would work, but is not necessary. Broadcaster Facility ID’s and cable system Physical System ID’s overlap a little. Most EAS monitoring sources are broadcast stations with unique call numbers. National Weather Service radio stations typically use an ID that identifies the weather office rather than the transmitter. Local government emergency agencies typically use a friendly string, e.g. NYCEOC. Cable and satellite systems typically use a corporate name, nationwide; but are rarely used as monitoring sources.

Interstitial alerts can occur for both valid and accidental reasons. Repeated header tones may accidentally occur when the audio of an EAS alert feedback into the transmission, such as during the 2011 National EAN Test. They also occur for valid alerts, such as a NWS radio site with a separate state/local EAS encoder installed in series with the NWS EAS encoder using NOAA Weather Radio Direct Audio Access (National Weather Service, 2004). If both a weather alert and local alert occur at the same time, the transmission line may be interrupted in mid-alert by the other alert. My understanding is most Primary Entry Point System stations install FEMA and local EAS encoders in series, which may result in a FEMA activation seizing the program line in mid-transmission of a local EAS alert. Those will also result in an incomplete local alert interstitial transmission.

The robustness principle implies EAS decoders and encoders should be prepared to handle interstitial alerts or risk losing Presidential alerts at PEP stations. The question is how should they handle it. I suggest EAS decoders should handle interstitial alerts in two ways:

1. If it detects duplicate headers from the current monitoring source, it should not interrupt the current alert. It should treat them as an audio echo.
2. If it detects new headers from the current monitoring source, it should terminate the current alert by transmitting an end-of-message(EOM). It should then process the new alert.

6.6. Confidentiality and Information Sharing

6.6.1. Information Sharing with Federal Partner Agencies

The Federal Communications Commission, Federal Emergency Management Agency, and National Weather Service are jointly responsible for the management of the Emergency Alert System at the federal level. At a minimum, all EAS management, operational, security and reporting-related details submitted to the FCC should be shared on a confidential basis between FCC, FEMA and NWS. And at a minimum, EAS operational status information should be shared on a confidential basis with potential users of EAS at the Federal level, i.e. the White House and other Federal agencies with emergency public information responsibilities in the National Response Framework, primarily ESF #2: Communications, ESF #5: Emergency Management and ESF #15: External Affairs. I consider EAS operational status information to be a subset of EAS information such as whether EAS is operating normally, degraded or not available so emergency officials will know to use other alert and warning systems.

Existing inter-agency Federal information sharing processes and agreements should be sufficient to protect EAS information, so special EAS Memorandums of Understandings should not be required between Federal agencies.

Federal agencies sometimes use open-ended information sharing language to avoid discussing law enforcement and national security information sharing. Because Federal law enforcement and intelligence agencies tend to have even more restrictive controls, I believe few EAS participants have significant concerns about information shared with Federal law enforcement and intelligence agencies for criminal and national security purposes. Due to the primary purpose the Emergency Alert System, transmitting a Presidential Alert, I expect most EAS participants assumed reports about EAS problems and malicious activity would already be shared with Federal law enforcement and intelligence agencies.

Information will also need to be shared with other Federal agencies with useful subject matter expertise. For example, that National Institute of Science and Technology, National Telecommunications and Information Administration, and cybersecurity programs at the Department of Defense and Department of Homeland Security may have expertise FCC should leverage to analyze EAS problems and incidents. What information needs to be shared will be incident and analysis dependent. Although the FCC is an independent regulatory agency, it shouldn't try to do everything itself in a separate silo. Due to never-ending re-organizations and unpredictability of what problems will need to be analyzed, identifying specific named Federal agencies is probably unwise. A general process should allow information sharing with other Federal agencies on a confidential basis for the purposes of analyzing incidents, problems and planning.

6.6.2. Information Sharing with State and Local Partner Governments

At a minimum, EAS operational status information for their geographic areas should be available to State, territorial, tribal and local government agencies with public alerting and warning responsibilities. I consider EAS operational status information to be a subset of EAS information such as whether EAS is operating normally, degraded or not available so emergency officials will know to use other alert and warning systems. This should be automatic, and not require extensive certifications or agreements.

There is a lot of variability between states, territories, tribal and local governments. Some are passive users or non-users of the Emergency Alert System. Others are active participants and operate portions of the EAS infrastructure, such as state relay backbone networks.

Following the same principles as with subject matter Federal agencies, the FCC should share information with State and Local partner governments with a need to know, and capable of protecting the confidentiality of the information should have access to the appropriate management, security and reporting details. It is difficult to pre-identify exactly which agencies. I expect most non-Federal government agencies will remain passive users of EAS, and will not exert the effort to complete FCC certifications. Agencies with public safety, alerting and warning responsibilities willing to go through certifications and agreements to gain access to additional EAS management, security and reporting details; are likely also active EAS participants and responsible for portions of the EAS infrastructure within their geographic jurisdiction. The FCC would retain the authority to reject or revoke access, if the access is misused or not relevant to the purpose of EAS.

6.6.3. Information Sharing with Other Entities

The FCC will need other entities to assist with management, analysis and operation of the EAS system. The FCC already has general rules for sharing information with other entities for the purposes of analysis and planning.

The National Coordinating Center for Communications watch floor is part of the Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC). The NCC watch floor operates 24x7x365 as the Telecommunications Information Sharing and Analysis Center (ISAC). The NCC can perform quick analysis of incidents and identify cross-industry attacks involving other communications sectors. This is applicable to EAS and WEA as well other notification systems such as reverse-911, SMS, social media. However, NCC does include competitors within the same industry. While FCC reports may be shared by default with the NCC to help identify trends and cross-sector attacks, because FCC is a regulatory agency, EAS participants should be able to request the NCC not share specific details with the NCC industry members.

In depth analysis of EAS incidents will likely requires combinations of different, industry-specific organizations. NCC is over weighted with telecommunication industry interests. Broadcast, cable, internet, satellite, and others each have their own groups. Being volunteer organizations, State and Local Emergency Communications Committees vary tremendously in their capabilities. There is currently no national equivalent EAS advisory committee. Due to the voluntary nature of SECC/LECC groups, expecting legal agreements for the participants will only discourage volunteering even more. The FCC may suggest EAS participants voluntarily share reports with their SECC/LECC, avoiding many confidentiality issues and legal agreements. EAS participants would decide which specific details they share with the SECC/LECC members.

6.6.4. Treatment of Certification-Related Information

The EAS certification requirements appear to be primarily an annual federally sponsored data collection. It appears to be less about the certification, and more about collecting information.

The annual filing of the certification should be public and included in the relevant public file or business records of the EAS participant. As described in section 6.5.1 Annual Certification, instead of focusing on only a few EAS items, certifying the self-inspection checklists may make more sense.

The additional information requested, such as alternative security measures, should be considered confidential, and purged when the following year's certification is submitted. Information about obsolete or corrected security measures should not be retained.

6.6.5. Treatment of Reporting-Related Information

Unlike the annual certification requirements, the EAS reporting requirements are triggered by specific public incidents.

As the FCC is aware, telecommunication outage reports (NORS) were public for over a decade. After one telecommunications company used the FCC outage reports in its advertising, there was significant industry pressure to make the outage reports confidential for business reasons. After the 9/11 terrorist attacks, the FCC made the reports confidential even though the public reports were invaluable in reports such as “The Internet Under Crisis Conditions: Learning from September 11” (National Academy of Sciences, 2003). The practice of making outage reports confidential just increased the burden on requestors. Now researchers and reporters must submit requests through the Freedom of Information Act to obtain access to outage reports, creating unnecessary bureaucratic hurdles.

Assuming the FCC sets, the reporting thresholds appropriately, most reports filed will be about EAS incidents which attract public interest due to the impact on the public. The news media and social media currently speculate about the reasons for false alerts and complain about EAS lockups. Lack of accurate information, which could be provided by the reporting requirements, just results in more speculation.

The electric industry used to keep power outage information confidential, claiming criminals would use it to commit crimes. In practice, criminals could see the lights were out. Many electric companies now post outage information on their web sites, and the National Electric Reliability Commission publish DAWG reports (Disturbance Analysis Working Group) on its web site. The electric industry found out publishing the outage information saved them money, because fewer people called their customer care centers asking about power outages and when would it be fixed.

EAS reporting information should not be presumptively treated as confidential. The basic information should be public, much like a power blackout; its already public it happened. The final report may have details which may require confidential treatment. Confidentiality should not be used to cover stupidity or delay fixing things. In cases involving the FDA and NHTSA, the lack of public disclosure has allowed manufacturers to defer fixing products for years. After a public disclosure occurred, manufacturers suddenly made progress addressing those vulnerabilities.

The Communications Security, Reliability and Interoperability Council V, Working Group 3, Emergency Alert System takes an old fashion approach from the 1990’s and recommends:

> “(1) Information about how EAS Participants have implemented the security best practices should not be a matter of public record and should be held confidential. The Commission should work with other federal agencies to establish processes for sharing information that is considered by EAS Participants to be sensitive and non-public.”

History has demonstrated that industries and organizations tend to de-prioritize and dismiss security and safety issues (i.e. risk acceptance) when those issues are kept non-public. There are very few “new” EAS security issues. The fact EAS security issues have not been addressed for years or even a decade in some cases is additional evidence of this. The CSRIC WG further recommends the confidential information should be voluntary, and the FCC should not take any enforcement action based on the information. While that is an expected position that industry and businesses will recommend, it also allows them to continue to do as little as possible. Health departments post letter grades for restaurants with food safety issues. Buildings are required to post signs when safety systems, such as fire alarms and sprinklers, are not working.

While keeping information about flaws in burglar alarms helps protect a company's property and assets, keeping information secret about flaws in public safety systems puts the public at risk. Instead of using a 1990's approach to computer security, where some companies sued security researchers for reporting flaws, a more modern approach is delayed disclosure. Security researchers notify the company, and after a reasonable amount of time (i.e. 90 days, 180 days) to allow the company to fix the problem, the flaws are publically disclosed. This provides incentives for security researchers to report problems and incentives for companies to fix those problems. Currently EAS Participants don't need to report any EAS equipment problems to the FCC for 60 days (11.35(b)), and as long as they "informally" notify the FCC, there is no maximum time limit on fixing equipment problems (11.35(c)). This provides EAS Participants time to quickly fix problems without needing to report to the FCC or risking any FCC enforcement action, and once fixed are no longer as sensitive.

The EAS is a public safety system. At a minimum, the FCC should report aggregated and anonymized information about the operational readiness, common issues and milestones to address problems in the EAS.

6.6.6. Confidentiality of Equipment Manuals and Commercially Available Information

Repeating that there are trade-offs between "security through obscurity" and "loose lips sink ships," expecting commercially available information such as equipment manuals and default configuration settings, e.g. default passwords, will remain confidential is unrealistic. Implementing industry-wide distribution controls, supply-chain security, and background investigations of all purchasers would likely be expensive and have a poor return on investment. While embedded system manufacturers have a learning curve how to ship products with default secure configuration settings, the experience of vendors trying to keep manuals and security vulnerabilities secret has been many presentations at DEFCON and other security conferences by security researchers.

Some large IT vendors like Cisco, Juniper and Microsoft made the business decision to provide security patches to everyone, even without support contracts or identification. Other vendors only provide security patches and updates to customers with active support contracts because they depend on the revenue from support contracts to pay programmers maintaining the software. It is important to recognize that vendors which require support contracts for security patches generally do so for business, not security reasons. An EAS manufacturer may choose to restrict its product manuals and other information. It should be their business decision, and not because the FCC is shielding them.

FEMA published a series of EAS Best Practices (Federal Emergency Management Agency, 2011) which included the default passwords for major EAS equipment manufacturers as part of the instructions.

Other Federal regulatory agencies have recently needed to addressed embedded software security in medical devices and automobiles. The Food and Drug Administration and National

Highway Traffic Safety Administration have generally focused on improving the security of products, not trying to keep product vulnerabilities secret.

6.6.7. Confidentiality of EAS Plans and Operational Details

By their nature, public alerting and warning systems are public.

The public needs to have confidence in the operation of the EAS system. Secret plans tend to decrease public confidence and increase conspiracy theories. Non-participants, such as hospitals, schools and industrial facilities sometimes integrate EAS messages as part of their local mass notification warning systems. Information such as monitoring sources and how to obtain EAS, IPAWS and Local/State CAP messages should be publically available. While most members of the public aren't interested in emergency plans until an emergency occurs, FEMA, state and local emergency management agencies generally publish their emergency plans with the exception of specific operational details such as authentication codes and tactical details. The FCC EAS Operating Handbook, National Weather Service directives for weather warnings, FEMA national warning procedures using EAS/CAP, State/Local EAS/CAP plans, and other EAS originators' plans like AMBER alerts should be public and include information how the public and participants can validate alerts.

Only some operational details, such as passwords used by government officials to verify their identity and specific tactical details, should be confidential. Since authentication passwords should be changed regularly, and only used between the individual government official and the EAS origination point, they normally would not be included in the published plans anyway. There may be some other tactical details which emergency officials believe should be in a non-public appendix. FCC should consult and learn from FEMA's experience about which tactical details should be treated as confidential.

6.7. Reach of Proposed EAS Security Rules

While the Emergency Alert System is a mandatory program, it relies on participants to voluntarily take on work in different roles. In the 1950's, 1960's, and 1970's, the government provided lots of carrots to encourage industry participation in those roles. The government provides few, if any carrots anymore. The greater cost and resource differential between roles, the more difficult it will be to find volunteers for the more difficult EAS roles.

6.7.1. EAN Only

Since the 1970's, the FCC has leveraged its national defense authorities to also create a shared state/local warning capability. Because EBS, and later EAS, participants already had to operate the equipment for national duties, using the same equipment for state/local alerts had minimal incremental cost. If EAS participants needed to voluntarily install separate equipment for state/local alerts, I suspect many would not. Although not required too, many major news stations have separate weather wire equipment, with more advanced capabilities such as nicer graphics and full text of the NWS information. They do not use EAS equipment for weather alerts, and therefore use much nicer sounding alert chimes.

As described earlier in sections 6.5.4 and 6.5.5, better specification of the EAN message and operation procedures would improve its security. However, the extreme rarity of EAN messages makes any Return on Investment calculation essentially meaningless. As much as possible, changes to the EAS protocol transmission should be done consistently for all alerts. The power of the EAN message, i.e. unlimited duration, lockout other programming, and nation-wide affect, could justify some additional software checks for just EAN messages as long as they can be performed automatically. But there should not be two different protocols: 1) EAN and 2) everything else.

When EAS, including EAN, eventually moves to digital distribution, I hope the current analog EAS protocol will be replaced for everything.

6.7.2. Exception for PN Station

Although PN participants and don't relay alerts to other EAS participants, the major network-affiliates and pay TV distribution systems are the primary source of alerts for the public. In terms of number of licensees, other broadcast radio/TV stations (PN) have less impact on public alerting. Local Primary and State Relay stations have outsized impact because of their role as downstream monitoring sources. Reducing the dependence on the EAS daisy-chain would also reduce that impact.

If the FCC makes exceptions, it should not be based on the EAS role. It should be based on the aggregate public impact the EAS participant plays in the EAS system. This reduces the arbitrage opportunity of participants not volunteering for particular roles. An EAS security issue at a small low-powered, educational broadcast radio with a small audience has much less impact than a national head-end in the sky serving millions of pay TV subscribers, even though both may have the role of PN participants in EAS. In some markets, all the LP stations are non-profit organizations with much smaller audiences. I don't know all the business reasons why some stations choose certain EAS roles.

6.7.3. Exception for Small Entities

This appears to be a variation on the old EBS Non-Participating National (NN) role. If the resulting proposal has fewer requirements and less expense, I expect small entities would be in favor whatever is proposed. It is reasonable that low-impact participants do not need the same expensive security controls. If small entities didn't carry the EAN message itself, would the small entity need to monitor EAS and informed its listeners/viewers to tune elsewhere for the EAN message? What would be the aggregate impact on the public? In aggregate across all the entities that didn't carry the EAN message, how many people would completely miss the alert, or learn about the warning through Wireless Emergency Alerts or some other alert application? If small entities still needed to monitor the EAS system and transmit a message about the EAN message, but they don't carry the actual EAN message like the old Non-Participating National role, would that actually save them money?

6.8. Preserving EAS Defense through Planned Diversity

The public is served by several public alerting systems in the U.S. In addition to government alert distribution systems, there is the traditional news media, social networks, and private alerting systems. They use multiple, diverse distribution channels including terrestrial broadcast, wireless, microwave, satellite, wireline, etc. While they may not be planned diversity, in combination they keep the public informed during most emergencies.

The over-the-air daisy-chain from Primary Entry Point System was originally a "last resort" system created in 1983 after the breakup of AT&T. Until 1995, national radio and TV networks (e.g. ABC, CBS, NBC, PBS, etc.) were envisioned as the primary distribution channel of Presidential messages through the Emergency Action Notification Network and their affiliates. After a series of government cost-cutting measures, the last resort over-the-air system became the only system for Presidential alerts through EAS.

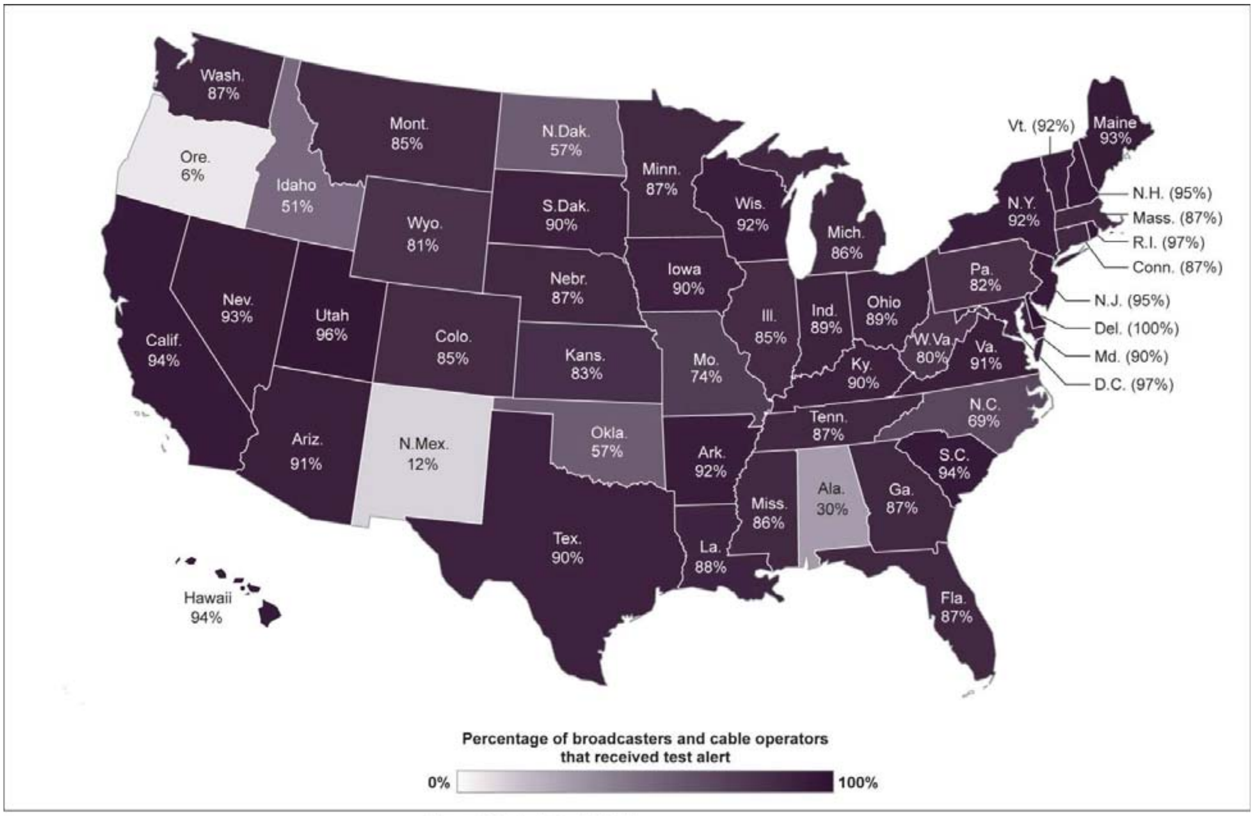
The Internet offers resiliency of transient failures, and recovery through alternate, available communications channels. Traditional telephone and radio communication protocols at the time required re-establishing a new call on a different channel to continue after a transient failure. Over-the-air EAS protocols do not recover without loss from an interrupted EAS transmission. However, the Internet was not designed to survive loss of all physical communications paths. When there is only a single "last-mile" connection to the EAS Participant, Internet protocols can't create a new physical connection from nothing. In "The Design Philosophy of Internet Protocols" (Clark, 1988), David Clark described the reasoning:

> "The most important goal on the list is that the Internet should continue to supply communications service, even though networks and gateways are failing. In particular, this goal was interpreted to mean that if two entities are communicating over the Internet, and some failure causes the Internet to be temporarily disrupted and reconfigured to reconstitute the service, then the entities communicating should be able to continue without having to reestablish or reset the high level state of their conversation. More concretely, at the service interface of the transport layer, this architecture provides no facility to communicate to the client of the transport service that the synchronization between the sender and the receiver may have been lost. It was an assumption in this architecture that synchronization would never be lost unless there was no physical path over which any sort of communication could be achieved. In other words, at the top of transport, there is only one failure, and it is total partition. The architecture was to mask completely any transient failure."

In November, 2011, FEMA and FCC conducted a "sunny-day" test, with extensive pre-notification and planning of the nation-wide capability of the Emergency Alert System. The Government Accountability Office analysis (Government Accountability Office, 2013) of FCC data found that approximately 82 percent of reporting broadcasters (radio and television) and cable operators received the November 2011 nationwide test alert. FEMA reported that 3 of the 63 PEP stations were unable to receive and retransmit the alert due to technical reasons.

These PEP stations were located in New Mexico, Alabama, and American Samoa. Failures at those stations significantly contributed to low national-level alert reception rates in those states and that territory. In particular, GAO's analysis of FCC data found that nearly 90 percent of broadcasters in New Mexico, almost 70 percent of broadcasters in Alabama, and 100 percent of broadcasters in American Samoa failed to receive the national-level alert.

The state-by-state nature of EAS planning means some States have only a single source of national EAS alerts. Only a few states implement cross-border relay network diversity, such as the National Capital Region. In states with a single National Primary (NP) source for the state; when a single NP was disrupted, essentially all national alert distribution in that State was interrupted.



Source: GAO Analysis of FCC data.

Figure 4 Percentage of Broadcasters and Cable Operators that Received the Nationwide EAS Test

6.8.1. Ensuring a Modern and Effective EAS Structure

The current EAS structure is a middle-to-middle architecture. The EAS structure begins AFTER official sources release a warning, and ends BEFORE the public receives the warning. While the middle-to-middle architecture partially reflects the limits of FCC's authority, it hinders the effectiveness of the warning system.

An advantage of the classic analog EAS AFSK protocol is compatibility with a wide variety of analog communication channels, including telephones (POTS), narrowband VHF, AM/FM and amateur radio; analog cable TV, and so on. The traditional EAS structure had more automated features than EBS, but usually assumed news stations have staff available and broadcasters would be the primary EAS operators. EAS doesn't not require official government warning sources have any special equipment. State/local officials could distribute warnings to the primary EAS station by teletype, calling, faxing or even knocking on the door.

A disadvantage of the classic analog EAS AFSK protocol is it uses the program audio channel. Which means every EAS message must interrupt normal programming to reach other EAS participants or the public. Without the audio portion of the message, the EAS headers alone tend to confuse the public. Only a single message at a time may be transmitted, and managing multiple channels can get complicated. Because EAS AFSK uses in-band signaling, it is vulnerable to normal program content accidently triggering EAS equipment. This is a classic system vulnerability, and one of the reasons why the telephone system changed to System Signally 7 using out-of-band signally. A former advantage, but now a disadvantage is interrupting the program channel means disrupting more members of the public than necessary.

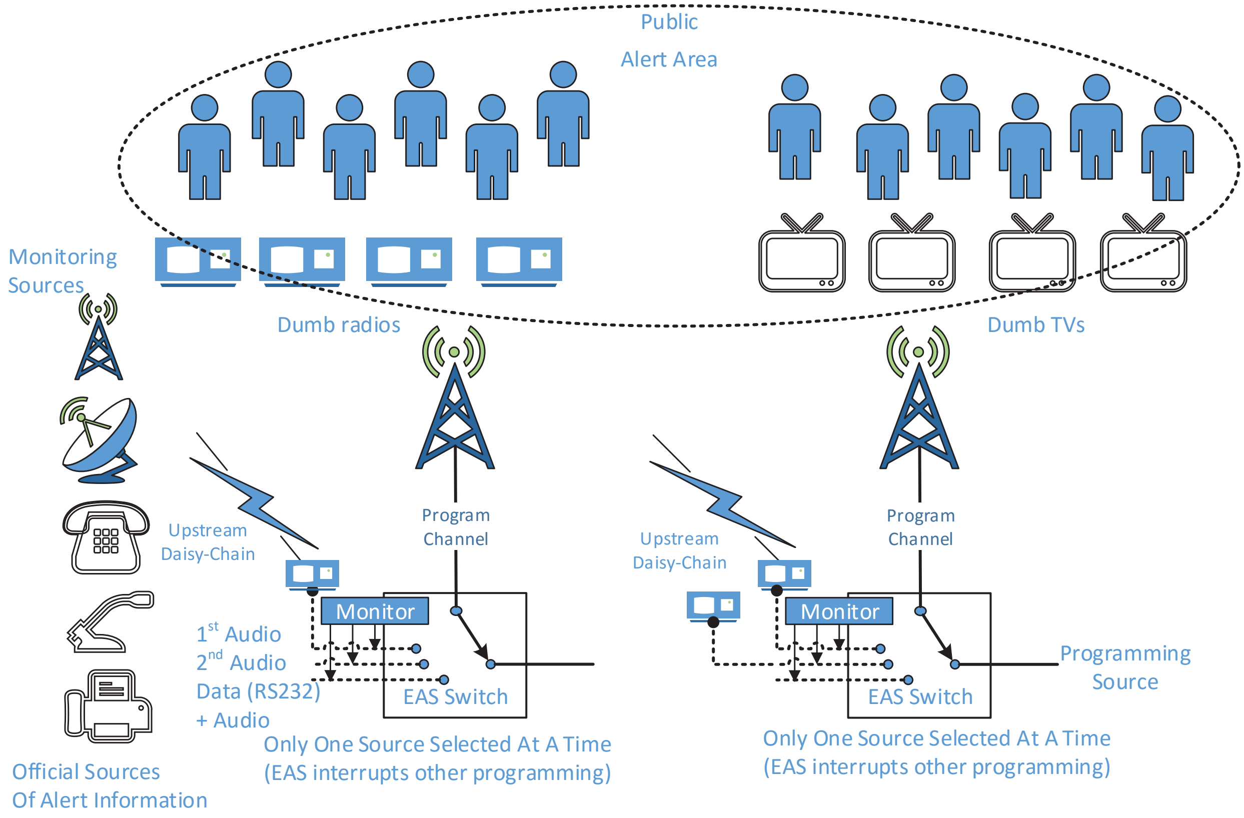


Figure 5 Classic EAS Distribution

For adequate diversity and resilience to a wide variety of disaster scenarios, multiple different communications technologies should be used. The classic EAS daisy-channel is low-cost and provides some redundancy. Although EAS was not used, in New York City on 9/11 and New Orleans during Hurricane Katrina, a combination of satellite, cable, internet and terrestrial broadcasters were needed because they experienced different types of damage. Eight New York City TV stations lost their over-the-air antenna on 9/11. During Hurricane Katrina, 50% of local radio stations and 44% of television stations went off the air. Even satellites have gone off the air, such as loss of control of Galaxy IV in 1998. Industry showed they could back each other up, but no single communications technology was superior in every case. According to Arbitron, during the 2004 hurricane season only about 52% of stations broadcast any EAS alerts, but 75% of the public reported hearing an EAS alert. (Arbitron Inc, 2005)

As much as possible, EAS should move from a daisy-chain distribution, to closed-circuit, point to multipoint distribution channels. FEMA, FCC and NWS should work with state/local emergency management agencies to directly originate and disseminate alerts to all EAS participants in the area instead of relaying through one or two broadcast stations in each area. That would reduce the dependency and risk on one or two LP stations in each area, and make verification simpler when the alert comes directly from the source agency. Using closed-circuit, point-to-multipoint also reduces the risk of other programming accidently triggering EAS equipment.

EAS participants with the greatest public impact, either due to market dominance or a key source for other participants, should have at least three different communication technologies for Presidential messages and state/local alerts, i.e. satellite, internet and terrestrial over-the-air. Fewer alternate communication technology channels or using the same communications technology for redundant channels may be justified for lower impact EAS participants, or potentially in remote areas with fewer alternatives. The impact on the public should be measured from the point of view of the public, not the distribution channel.

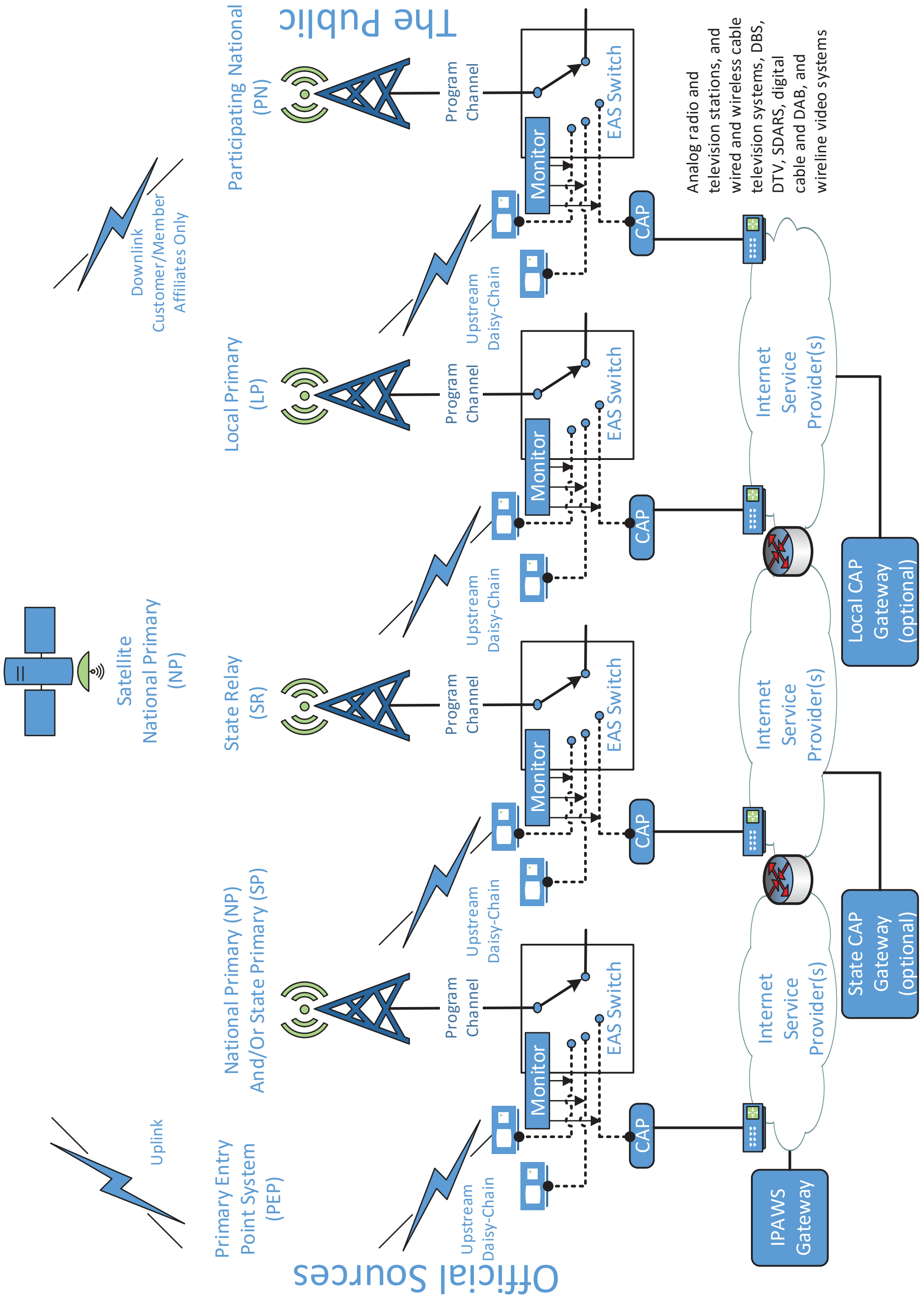

Official Sources
Primary Entry Point System (PEP)
Uplink
Satellite National Primary (NP)
Downlink Customer/Member Affiliates Only
National Primary (NP) And/Or State Primary (SP)
State Relay (SR)
Local Primary (LP)
Participating National (PN)
The Public
Upstream Daisy-Chain
Upstream Daisy-Chain
Upstream Daisy-Chain
Upstream Daisy-Chain
Upstream Daisy-Chain
Program Channel
Program Channel
Program Channel
Program Channel
Monitor
Monitor
Monitor
Monitor
EAS Switch
EAS Switch
EAS Switch
EAS Switch
CAP
CAP
CAP
CAP
Analog radio and television stations, and wired and wireless cable television systems, DBS, DTV, SDARS, digital cable and DAB, and wireline video systems
Internet Service Provider(s)
Internet Service Provider(s)
Internet Service Provider(s)
IPAWS Gateway
State CAP Gateway (optional)
Local CAP Gateway (optional)

Figure 6 Current EAS Distribution

If EAS was designed from scratch today, it should use a digital transport protocol, including the message portion besides the headers; with satellite as the primary distribution channel, Internet as a secondary distribution channel, and terrestrial TV broadcasters as a tertiary distribution channel. Satellites can cover most of the country, with higher bandwidth supporting audio, video and data. Internet supports two-way communications to support status reporting and backup alert distribution, over almost any digital data transport. Digital TV stations and digital cable also have high-bandwidth, digital channels. Analog channels, such as AM radio and analog cable would be leaf nodes, at the end of the distribution tree. End-to-end digital transport using control channels eliminates the problems of program content accidently triggering EAS equipment. End-to-end digital transport also enables smart devices and more user control over which alerts interrupt their activities.

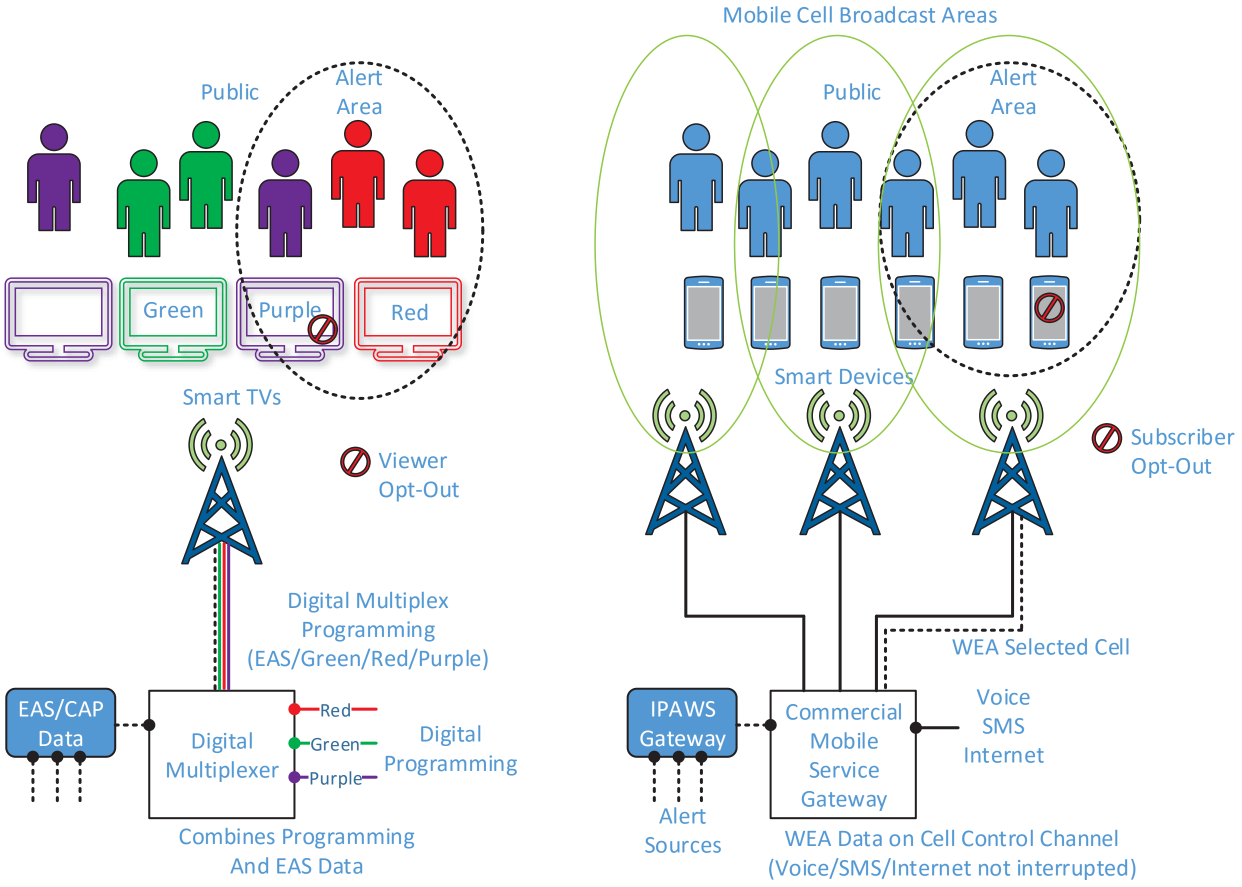


Figure 7 Future Alert Distribution

6.8.2. Securing the EAS Broadband Architecture

Internet broadband is a two-way public network. Internet broadband networks can be attacked by anyone in the world. EAS, and EBS, were developed in mostly one-way, closed circuit distribution networks. Closed circuit networks have less exposure to outside attacks, but are sometimes crunchy, candy shells; with no internal security. Because the classic EAS closed circuit design has very little internal security, it is vulnerable to channel attacks, network attacks, equipment attacks and operator attacks. EAS equipment which was traditionally in a closed environment is now more exposed with CAP, and EAS manufacturers and EAS participants must adapt to the new threat environment.

Understanding the different environments is important to understanding different ways to keep them secure.

DHS and the NCC have performed telephone network dependency analysis in the past, and may be able to work with the FCC to analyze the various radio route dependencies in the EAS system. Conducting both lab tests, and red teams on the CAP systems is also necessary. Whether or not the FCC does its own testing, with anything connected to the Internet, it’s almost guaranteed other people are, and not informing the FCC of their findings.

The EAS/CAP systems need to be operational while the EAS participant is operating. If the FCC has requirements for an EAS participant to stay on the air, then the EAS/CAP systems at that participant should meet the same requirements. On the other hand, if the FCC has no business continuity requirements for a station to stay on the air; while they are off the air the status of the EAS/CAP systems don’t matter.

A. Hypothetical EAS Registration Form

Note: The online form should pre-populate information from FCC and other databases, e.g. US postal information, Census/USGS location names, FCC/FEMA/SECC/LECC curated lists of EAS information, etc. and perform data quality checks. Bulk uploading of information for organizations with many facilities should be supported. Registration information from previous registrations should be carried forward for updating and not need to be re-entered every year and each registration.

1. EAS Participant Information.

Enter the name, FCC Registration Number (if available) and mailing address of EAS Participant.

Legal Name		FCC Registration No. (FRN)	
Assumed/doing business as (dba) Name			
Mailing Address	City	State	ZIP Code

2. Points of Contact.

Administrative Contact. Enter the name, telephone number (including area code), and e-mail address of the person responsible for questions regarding this form.

Name of Administrative Contact	Telephone No.	E-mail Address

Technical Contact. Enter the name, telephone number (including area code), and e-mail address of the EAS technical representative for the participant.

Name of EAS Technical Contact	Telephone No.	E-mail Address

3. Identification of EAS Communication Facility.

FCC Identifier of Facility. Enter the FCC Identifier of the communication facility which will transmit EAS alerts. The Type of Facility specifies the appropriate database source of FCC identifiers, and does not necessarily reflect the FCC regulatory category of the participant. Other Entities should coordinate with FCC, SECC or LECC to choose unique Identifiers for the participant's facilities (i.e. each communication facility with EAS equipment).

EAS ID (LLLLLLLL code) must match the code transmitted by the participant's EAS equipment. If a facility has multiple EAS encoders, e.g. NOAA transmitters with both NOAA SAME encoders and State/local EAS encoders, submit separate EAS Registration Forms with the same Identifier and distinct EAS ID's.

Type of Facility	**Use this identifier (FCC DB)**	**Identifier**	**EAS ID (LLLLLLLL code)**
Broadcast Service	Facility ID No. (CDBS/LMS)		
Cable Service	Comm. Unit/NC ID (COALS)		
CAP Aggregator	CAP Gateway Name		
NOAA Weather Radio	Call Sign (NTIA)		
Satellite Service	Call Sign (IBFS)		
Wireless Service	Call Sign (ULS)		
Wireline Service	CLLI Code (Telcordia)		
Other Entity	Call Sign/ID Code/Name		

EAS Common Name. Enter a common name for this communication facility, e.g. call sign, site name, agency name, etc. This should be a meaningful name to distinguish different EAS participants sharing the same communications facility or groups of communication facilities operated as the same EAS participant. Some examples include a broadcast station with multiple translator/booster stations, a regional cable system serving multiple communities, a weather forecast office operating multiple weather radio transmitters, a Primary Entry Point station with both FEMA equipment and its own EAS equipment sharing the same transmitter, a network program supplier with multiple distribution channels, a government agency better known by a different name, and so on.

EAS Common Name:

Monitoring Instructions. If other EAS Participants or the general public require additional information to monitor this EAS source, e.g. a specific channel, secondary audio channel, etc.; provide instructions.

Monitoring instructions for downstream EAS Participants (if applicable):

4. Joint facilities sharing common EAS equipment.

List EAS communication facilities which share this EAS Equipment for transmitting alerts. Enter a Type of Facility, Identifier, EAS ID and Common Name (e.g. call sign, site name, agency office, etc.) The communication facilities may share the same or have different EAS IDs.

This description does not change any regulatory requirements about sharing EAS equipment or specify a particular physical/virtual EAS architecture or implementation. For example, participants may operate additional transmitters (boosters, translators or repeaters), community unit IDs connected through the same physical system, non-cable community IDs, satellite stations, wireline offices, etc. with a common control point, head-end, hub office, studio, etc. Participants may indicate independently operated individual facilities or jointly operated common facilities by submitting separate EAS registration forms and/or combined EAS registration forms which most accurately reflects its EAS operations. EAS communication facilities with multiple sets of EAS equipment controlled by different entities, such as Primary Entry Point Systems with both FEMA and broadcaster EAS equipment, should file separate EAS registration forms for each set of EAS equipment.

Type of Facility	**Identifier**	**EAS ID (LLLLLLLL code)**	**EAS Common Name**

Add more lines as needed.

5. Regulatory Class of Participant. May check more than one box.

Check the regulatory classes of this EAS communication facility. This includes both required and optional classes of EAS participants.

☐Analog radio broadcast station

☐Analog television station

☐Analog cable system

☐Digital audio broadcasting (DAB) station

☐Digital television station

☐Digital cable system

☐Satellite Digital Audio Radio Service (SDARS)

☐Direct Broadcast Satellite (DBS) service

☐Satellite Master Antenna TV (SMATV) system

☐Wireless cable system ☐Wireline video system ☐Other Multichannel Video Program Distributor (MVPD)

☐Government entity ☐Network program supplier ☐Other participating entity

6. EAS Designation of Participant. May check more than one box.

Check the EAS Designation(s) of this EAS communication facility. Only check Participating National (PN) if this facility monitors required key EAS sources and relays required National EAS alerts including EAN, NPT and RMT. Optional EAS Participants in the National EAS should also check Optional Participant (OP). Participants which only participate in the National EAS, and not a State/Local EAS, should also check National Only (NO). Participants which originate EAS alerts, not including EAS testing such as DMO, RMT and RWT, should also check Alert Originator (AO).

☐Participating National (PN) ☐Local Primary (LP) ☐Local Relay Network (LRN)

☐State Relay (SR) ☐State Primary (SP) ☐State Relay Network (SRN)

☐National Relay (NR) ☐National Primary (NP) ☐Interstate Relay Network (IRN)

☐Alert Originator (AO) ☐National Only (NO) ☐Optional Participant (OP)

7. Location of Participant.

Enter community name (i.e. community of license, community unit, hub location, etc.), county, state, and 5-digit FIPS/ANSI location code (SSCCC) of the participant. This should be the location programmed in the EAS equipment for non-geographic participants and remotely operated EAS equipment. Additional locations served are listed in question #8 below.

Name of Community	County/Parish/Borough	State	FIPS/ANSI

8. Intended Service Area and Alert Audience.

List the 6-digit FIPS/ANSI EAS PSSCCC location codes for each State/county-equivalent with an audience the participant intends to alert, including the participant's own location from question #7. This should include all audiences alerted by the EAS communication facility in question #3 plus all jointly operated EAS communication facilities listed in question #4.

IMPORTANT: The participant's intended service area and alert audience may be different than the State/counties within a Local EAS Area's boundaries. This is also not necessarily the same as the "incoming filters" programmed in the EAS equipment. Do not list State/county codes on the fringe of the participant’s signal or state-wide codes unless the participant intends to alert the audience in those counties or state-wide directly or indirectly through an EAS daisy-chain (i.e. the State Primary or Local Primary station). If only a small portion of a large county/county-equivalent is the intended service area and alert audience, participants may use the P-portion code. For state-wide service areas and alert audiences, list the state-wide code (i.e. 0SS000). National/satellite providers list each state and territory with an alert audience, do not use the nation-wide code 000000 (six zeros).

9. Local EAS Operational Area.

Enter the name of the Local EAS Operational Area as defined in the State EAS Plan or Monitoring Assignment letter. Usually based on the State and county of the EAS Participant in question #7, but some EAS boundaries split counties/county-equivalents into separate Local EAS Operational Areas or adjacent States. An EAS Participant may be assigned to a different EAS area for monitoring and community service reasons. Non-geographic EAS Participants should enter the Local EAS Operational Area used for Required Monthly Tests and EAN monitoring.

Name of Local EAS Operational Area	State

10. EAS codes originated and relayed.

Check the originator code used by this EAS communication facility.

☐ CIV Civil authority	☐ EAS EAS participant	☐ PEP Primary Entry Point System	☐ WXR National Weather Service	☐ None Decoder only

Check each event code Originated (“☐O”) and Relayed (“☐R”) by this EAS communication facility. Although EAS Participants may originate or relay any optional event code, do not check event codes the participant does not plan to originate or relay.

National Event Codes (Required)							
EAN☐O ☒R	NIC☐O ☒R	NPT☐O ☒R	RMT☐O ☒R	RWT☒O ☐R			
State/Local Event Codes (Optional)							
ADR☐O ☐R	AVA☐O ☐R	AVW☐O ☐R	CAE☐O ☐R	CDW☐O ☐R	CEM☐O ☐R	DMO☐O ☐R	EQW☐O ☐R
EVI☐O ☐R	FRW☐O ☐R	HMW☐O ☐R	LAE☐O ☐R	LEW☐O ☐R	NMN☐O ☐R	NUW☐O ☐R	RHW☐O ☐R
SPW☐O ☐R	TOE☐O ☐R	VOW☐O ☐R					
Weather Event Codes (Optional)							
BZW☐O ☐R	CFA☐O ☐R	CFW☐O ☐R	DSW☐O ☐R	EWW☐O ☐R	FFA☐O ☐R	FFS☐O ☐R	FFW☐O ☐R
FLA☐O ☐R	FLS☐O ☐R	FLW☐O ☐R	HLS☐O ☐R	HUA☐O ☐R	HUW☐O ☐R	HWA☐O ☐R	HWW☐O ☐R
SMW☐O ☐R	SPS☐O ☐R	SSA☐O ☐R	SSW☐O ☐R	SVA☐O ☐R	SVR☐O ☐R	SVS☐O ☐R	TOA☐O ☐R
TOR☐O ☐R	TRA☐O ☐R	TRW☐O ☐R	TSA☐O ☐R	TSW☐O ☐R	WSA☐O ☐R	WSW☐O ☐R	

11. Key EAS sources monitored.

List Key EAS sources monitored by this EAS communication facility. Mandatory EAS Participants must monitor two EAS sources plus the FEMA IPAWS gateway. If monitoring a different key EAS source than required by the applicable National, State or Local EAS Plan or received a Monitoring Assignment waiver, check the exception box and provide the reason. EAS Participants may monitor additional EAS sources and CAP gateways. Participants may have other EAS activation methods using special sources which don't use the EAS AFSK protocol such as fax, remote control, and manual phone patches.

The Type of Facility and Identifier should match that source's answers for question #3 on their registration form to enable correlating upstream sources and downstream monitors for the map book. Pre-populated based on SECC/LECC curated list for the local EAS operational area.

Monitoring Source	**Type of Facility**	**Identifier**	**Exception/Reason**
CAP #1: FEMA	CAP Aggregator	IPAWS	☐
CAP #2: Optional	CAP Aggregator		☐
CAP #3: Optional	CAP Aggregator		☐
Source #1: Required			☐
Source #2: Required			☐
Source #3: Optional			☐
Source #4: Optional			☐
Source #5: Optional			☐
Source #6: Optional			☐
Special #1: Optional			☐
Special #2: Optional			☐
Special #3: Optional			☐

12. (FOUO) <u>EAS equipment</u>.

Enter the manufacturer, model number and software version used by this EAS communication facility. If no EAS Encoder or no CAP functionality, enter "NONE" for EAS Encoder or CAP Intermediary equipment. If EAS Encoder and/or CAP Intermediary equipment is integrated with EAS Decoder, enter "N/A" for EAS Encoder or CAP Intermediary equipment.

EAS Decoder (and ☐ Encoder, and ☐ CAP) manufacturer	Model Name/Number	Software Version
EAS Encoder equipment manufacturer	Model Name/Number	Software Version
CAP Intermediary equipment manufacturer	Model Name/Number	Software Version

13. (FOUO) Operational Readiness Checklist.

Participating National (PN) and voluntary national level EAS participants must complete the following national level EAS operational readiness checklist for the EAS communication facility registered on this form.

“Yes” means the EAS communication facility is in compliance with the question. “Pending” means the EAS communication facility is not in compliance with the question. Corrective action is pending. “N/A” means the question is not applicable to the EAS communication facility.

Compliance	**National Level EAS Operational Readiness Question**
☐Yes ☐Pending ☐N/A	1. Participating National: Is this EAS communication facility categorized as a Participating National (PN) source (§ 11.41) or voluntarily participates in the national level EAS? (§ 11.43) Entities not participating in the national level EAS may check N/A and do not need to complete the operational readiness checklist.
☐Yes ☐Pending	2. Certified Equipment: Does the participant use only certified EAS equipment (i.e. decoder, encoder and/or CAP intermediary device) at each location utilized for EAS operations? (§ 11.34)
☐Yes ☐Pending	3. Equipment Status: Is the required EAS equipment installed in accordance with the manufacturer’s instructions and in operational condition? (§ 11.35)
☐Yes ☐Pending	4. Equipment, Network and Software Security: Does the participant maintain the security of their EAS equipment, software and network connections; and mitigate known security vulnerabilities? (§ 11.35) Check each of the following when compliant: ☐ Protect against unauthorized access ☐ Defense in depth ☐ Remediate identified vulnerabilities ☐ Incident response plan ☐ CAP digital signature validation

☐Yes ☐Pending	5. Monitoring Assigned EAS Sources: Are the EAS receivers tuned to receive EAS activations from the required two key EAS sources or this EAS communication facility has a Monitoring Assignment waiver? (§ 11.52)
☐Yes ☐Pending	6. Monitoring Assigned CAP Source: Is the EAS equipment (or CAP intermediary device) configured to receive CAP activations from the required FEMA IPAWS gateway or this EAS communication facility has a Monitoring Assignment waiver? (§ 11.52)
☐Yes ☐Pending ☐N/A	7. Instantaneous Alert Reception: For manually operated EAS equipment, is the equipment installed in a way that alerts responsible staff instantaneously upon receipt of a valid activation during all operating hours? Participants using only automatic operation may check N/A. (§ 11.52)
☐Yes ☐Pending ☐N/A	8. Automatic Operation: During periods of unattended operation, is the EAS equipment configured to automatically interrupt programming? Participants with responsible staff on duty during all operating hours and using manual operation may check N/A. (§ 11.52)
☐Yes ☐Pending ☐N/A	9. Equipment Location: For manually operated equipment, is the EAS equipment positioned where responsible staff can immediately initiate an activation during all operating hours? Participants not required to have EAS encoders may check N/A. (§ 11.51)
☐Yes ☐Pending	10. Emergency Action Notification: Is the participant prepared to immediately interrupt normal programming, either automatically or manually, upon receipt of a valid national Emergency Action Notification (EAN) message and perform EAS operations during a National Level Emergency? (§ 11.54)
☐Yes ☐Pending ☐N/A	11. Weekly Testing: Does the participant transmit the required weekly test consisting of the EAS header and EOM codes a minimum of once a week, or an EAS activation in lieu of a required weekly test? Participants not required to have EAS encoders may check N/A, but still must log required weekly tests received. (§ 11.61(b))

☐Yes ☐Pending	12. Monthly and National Testing: Does the participant transmit the required monthly test, or national periodic test or EAS activation in lieu of a require monthly test, consisting of the EAS header, two-tone attention signal, audio (and video if applicable) message and EOM codes? Participants not required to have EAS encoders must transmit the test script. If the participant is not operating at the time a required monthly or national periodic test is scheduled, they shall log that they were not operating at that time and follow their weekly testing requirements during that week when operations resume. (§ 11.61(a) and (c))
☐Yes ☐Pending	13. EAS Logs Maintained: Does the participant maintain a log containing an entry of all EAS events sent and all national level alerts, required tests (NPT's, RMT's, RWT's) and preselected state and local events received? (§ 11.35(a), 11.52(e)(2), 11.54(a)(3), 11.55(c)(7), 11.55(d)(4) and 11.61)
☐Yes ☐Pending	14. Failure to Receive EAS Test: Does the participant's log contain appropriate entries indicating the reasons why required EAS weekly/monthly/national test transmissions were not received? If all tests have been received and logged during the last two-year period, then the appropriate response is "Yes". (§ 11.35(a))
☐Yes ☐Pending	15. Equipment Outage: Does the participant's log contain appropriate entries documenting the date and time any EAS equipment was removed and/or restored to service? If there have been no such outages in the last two years, then the appropriate response is "Yes". (§ 11.35(b))

(FOUO) Corrective Action and Milestones. Provide a corrective action and target completion date for each pending item in the national level EAS operational readiness checklist.

Corrective Actions and Target Completion Dates:

Add more lines as needed.

B. Suggested EAS Protocol and Rule Improvements

§ 11.31 EAS protocol.

(a) The EAS uses a four-part message for an emergency activation of the EAS. The four parts are: Preamble and EAS Header Codes; audio Attention Signal; message; and, Preamble and EAS End of Message (EOM) Codes.

(1) The Preamble and EAS Codes must use Audio Frequency Shift Keying at a rate of 520.83 bits per second to transmit the codes. Mark frequency is 2083.3 Hz and space frequency is 1562.5 Hz. Mark and space time must be 1.92 milliseconds. The message Header and EOM data is transmitted as 8-bit bytes, with no start or stop bits, using American National Standards Institute (ANSI) standard, ANSI INCITS 4-1986 ("Information Systems - Coded Character Sets - 7-Bit American National Standard Code for Information Interchange (7-Bit ASCII)") and the eighth (8th) bit set to one or zero.

(2) The Attention Signal must be made up of the fundamental frequencies of 853 and 960 Hz. The two tones must be transmitted simultaneously. The Attention Signal must be transmitted after the EAS header codes when including a message.

(3) The message may be audio, video or text.

(b) EAS Header and EOM Codes must be ASCII printable characters from ASCII 32 (space) to ASCII 126 (tilde). The ASCII 43 (plus) and ASCII 45 (hyphen-minus) symbols are required code element separators and must not be used within code elements. In lieu of a hyphen, call signs must use the ASCII 47 (slash) or other allowed punctuation character. Unused characters must be ASCII 32 (space) characters.

(c) The EAS protocol, including any codes, must not be amended, extended or abridged without FCC authorization. The EAS protocol and message format are specified in the following representation.

```
[PREAMBLE]ZCZC-ORG-EEE-PSSCCC+TTTT-JJJHHMM-LLLLLLLL-YYYY-
(one second pause)
[PREAMBLE]ZCZC-ORG-EEE-PSSCCC+TTTT-JJJHHMM-LLLLLLLL-YYYY-
(one second pause)
[PREAMBLE]ZCZC-ORG-EEE-PSSCCC+TTTT-JJJHHMM-LLLLLLLL-YYYY-
(at least a one second pause)
(transmission of 8 to 25 seconds of Attention Signal)
(transmission of audio, video or text messages)
(at least a one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(at least one second pause)
```

EAS Code Element Definitions:

[PREAMBLE] A consecutive string of bits (sixteen bytes of AB hexadecimal [8-bit byte 10101011]) sent to clear the system, set AGC and set asynchronous decoder clocking cycles. The preamble must be transmitted before each header and End of Message code.

ZCZC- The four exact ASCII characters ZCZC indicate the start of ASCII code.

ORG- Originator Code. Originator codes are three-letter, case-sensitive, codes that identify the organization type which originally initiated the activation of the EAS. The codes are specified in paragraph (d) of this section.

EEE- Event Code. Event codes are three-letter, case-sensitive, codes that identify the nature of the event or emergency that is causing the EAS activation. The codes are specified in paragraph (e) of this section.

PSSCCC- Location Code. Location codes are six-digit codes that identify which geographic areas may be affected by an emergency message. There must be from 1 to 31 Location codes in an EAS header. The codes are specified in paragraph (f) of this section.

+TTTT- Valid Time. Valid Time periods are four-digit time intervals that indicate the valid duration of a message. The time interval +TTTT contains two-digit hours +TT, from 00 to 99, and two-digit minutes TT in 15 minute segments up to one hour and then in 30 minute segments beyond one hour; i.e., + 0015, + 0030, + 0045, + 0100, + 0430 and + 0600. For EAN messages only, the time interval is also the minimum elapsed time before permitting an automatic EAS decoder reset, so lengthy Presidential alert messages can be handled.

JJJHHMM- Originator Daytime. Originator Daytimes indicate day of year and time when the message was initially released by the message originator. JJJHHMM contains the three-digit day of year JJJ, from 001 through 365 or 366 in leap years, and the time of day in two-digit hours HH and two-digit minutes MM using 24-hour Universal Coordinated Time (UTC). Valid EAS messages shall be considered as “For Immediate Release” and not embargoed because the Originator Daytime is in the near future.

LLLLLLLL- ID Stamp. Identification Stamps are eight-character, case-sensitive, codes (not including ASCII dash and plus symbols, unused characters must be ASCII space characters) that identify the message originator transmitting, or EAS Participant re-transmitting, the message. The ID Stamp will be automatically affixed to all outgoing messages by the EAS encoder.

YYYY- Originator Year. Originator Years indicate the year when the message was initially released by the message originator. YYYY contains the four-digit year. For compatibility with WRSAME and legacy EAS devices, the YYYY and trailing hyphen may not be present in messages originated or relayed through legacy monitoring sources. The EAS header is considered syntactically valid with and without an Originator Year YYYY. When an Originator Year is not present, the implied year shall be the Originator Daytime rounded up or down to the nearest year. For example, when the current date-time is in January, an Originator Daytime day-of-year JJJ = 365 implies the Originator Year is the previous year. Or for example, when the current date-time is in December, an Originator Daytime day-of-year JJJ = 001 implies the Originator Year is the next year.

NNNN The End of Message (EOM) code sent as a string of four ASCII uppercase N characters.

(d) The Originator code ORG indicates the organization type which initiated the message. Originator descriptions are informative, and may be translated into different languages or improved for clarity. Only the following Originator codes are presently authorized:

ORG code	**Originator description**
CIV	Civil authority
EAS	EAS participant
PEP	Primary Entry Point System
WXR	National Weather Service

(e) The Event code EEE indicates the nature of the EAS activation. This list includes codes for national EAS events and tests, which EAS Participants are required to receive and transmit; and codes for administrative, state and local, and weather EAS events, which EAS Participants voluntarily participating in state and local area EAS plans may receive and transmit on an optional basis. Only FEMA designated EAS sources, i.e. PEP stations and IPAWS gateways, are authorized to activate the national EAS using the Emergency Action Notification (EAN) event code. The nature of activation description is informative, and may be translated into different languages or improved for clarity. EAS equipment must support adding new Event codes. Only the following Event codes are presently authorized:

EEE code	**Nature of activation**
National Codes (Required):	
EAN	Emergency Action Notification (National only)
NIC	National Information Center
NPT	National Periodic Test
RMT	Required Monthly Test

RWT	Required Weekly Test
Administrative Codes (Optional):	
DMO	Practice/Demo Warning
NMN	Network Message Notification
State and Local Codes (Optional):	
ADR	Administrative Message
AVA	Avalanche Watch
AVW	Avalanche Warning
CAE	Child Abduction Emergency
CDW	Civil Danger Warning
CEM	Civil Emergency Message
EQW	Earthquake Warning
EVI	Evacuation Immediate
FRW	Fire Warning
HMW	Hazardous Materials Warning
LAE	Local Area Emergency
LEW	Law Enforcement Warning
NUW	Nuclear Power Plant Warning
RHW	Radiological Hazard Warning
SPW	Shelter in Place Warning
TOE	911 Telephone Outage Emergency
VOW	Volcano Warning
Weather Codes (Optional):	
BZW	Blizzard Warning
CFA	Coastal Flood Watch
CFW	Coastal Flood Warning
DSW	Dust Storm Warning
EWW	Extreme Wind Warning

FFA	Flash Flood Watch
FFS	Flash Flood Statement
FFW	Flash Flood Warning
FLA	Flood Watch
FLS	Flood Statement
FLW	Flood Warning
HLS	Hurricane Statement
HUA	Hurricane Watch
HUW	Hurricane Warning
HWA	High Wind Watch
HWW	High Wind Warning
SMW	Special Marine Warning
SPS	Special Weather Statement
SSA	Storm Surge Watch
SSW	Storm Surge Warning
SVA	Severe Thunderstorm Watch
SVR	Severe Thunderstorm Warning
SVS	Severe Weather Statement
TOA	Tornado Watch
TOR	Tornado Warning
TRA	Tropical Storm Watch
TRW	Tropical Storm Warning
TSA	Tsunami Watch
TSW	Tsunami Warning
WSA	Winter Storm Watch
WSW	Winter Storm Warning

(f) The Location code PSSCCC has three separate parts which hierarchically defines a specific geographic area. All three parts must be combined to identify each geographic area affected by an EAS activation, as specified in paragraphs (1), (2), (3) and (4) below. Location descriptions and abbreviations are informative, and may be translated into different languages or improved for clarity. EAS equipment must support adding new Location codes. EAS equipment must not reject messages which also contain undefined or unknown Location codes.

(1) The “SS” portion of the location code is a two-digit code that identifies the state or equivalent geographic area affected by an EAS activation. The “SS” code 00 (zero-zero) refers to the United States. “SS” codes for individual States, Territories and Freely Associated States are defined by American National Standards Institute (ANSI) standard, ANSI INCITS 38-2009 (“Information technology - Codes for the Identification of the States and Equivalent Areas within the United States, Puerto Rico, and the Insular Areas”). “SS” codes for individual Coastal and Offshore Marine Areas are defined by National Weather Service Instruction, NWSI 10-302 (“Marine and Coastal Services Areas of Responsibility”), Coastal and Offshore Marine Codes Listings for EAS and NWR Applications.

For convenience, the current “SS” codes used by the EAS protocol are listed in the following table.

SS Code	Abbreviation
00	US (National only)
States and District of Columbia:	
01	AL
02	AK
04	AZ
05	AR
06	CA
08	CO
09	CT
10	DE
11	DC
12	FL
13	GA
15	HI
16	ID

17	IL
18	IN
19	IA
20	KS
21	KY
22	LA
23	ME
24	MD
25	MA
26	MI
27	MN
28	MS
29	MO
30	MT
31	NE
32	NV
33	NH
34	NJ
35	NM
36	NY
37	NC
38	ND
39	OH
40	OK
41	OR
42	PA
44	RI
45	SC

46	SD
47	TN
48	TX
49	UT
50	VT
51	VA
53	WA
54	WV
55	WI
56	WY
Territories and Freely Associated States:	
60	AS
64	FM
66	GU
68	MH
69	MP
70	PW
72	PR
74	UM
78	VI
Coastal and Offshore Marine Areas:	
57	Eastern N. Pacific Ocean
58	N. Pacific Ocean Near Alaska
59	Central Pacific Ocean
61	S. Central Pacific Ocean
65	Western Pacific Ocean
73	Northwest N. Atlantic Ocean
75	West N. Atlantic Ocean

77	Gulf of Mexico
91	Lake Superior
92	Lake Michigan
93	Lake Huron
94	Lake St. Clair
96	Lake Erie
97	Lake Ontario
98	St. Lawrence River

(2) The “CCC” portion of the location code is a three-digit code that identifies the individual county or equivalent geographic area within the “SS” area affected by an EAS activation. The “CCC” code 000 (zero-zero-zero) refers to all counties or equivalent areas within a “SS” area. “CCC” codes for individual counties and some cities are defined by American National Standards Institute (ANSI) standard, ANSI INCITS 31-2009 (“Information technology - Codes for the Identification of Counties and Equivalent Areas of the United States, Puerto Rico, and the Insular Areas”). “CCC” codes for individual coastal and offshore marine areas are defined by National Weather Service Instruction, NWSI 10-302 (“Marine and Coastal Services Areas of Responsibility”).

(3) The “P” portion of the location code is a one-digit code that allows the message originator to divide an area identified by “SSCCC” into nine sections to further pinpoint the affected area. The “SSCCC” area may be an individual State/county (“SS” is non-zero and “CCC” is non-zero) or the entire State (“SS” is non-zero and “CCC” = 000). The “P” code 0 (zero) refers to all or an unspecified portion of an “SSCCC” area. The use of “P” codes for portions or subdivisions will probably be rare and generally for oddly shaped or unusually large “SSCCC” areas. Local EAS plan participants may coordinate State/county subdivisions in the State or Local EAS Map book. In the absence of a local process or procedure to define subdivisions, the following P codes may be used: 1 = Northwest, 2 = North, 3 = Northeast, 4 = West, 5 = Central, 6 = East, 7 = Southwest, 8 = South, 9 = Southeast.

(4) The Location code “PSSCCC” = 000000 (six zeros) identifies an EAS activation affecting the entire United States. No other “CCC” county or “P” portion codes are authorized for use with the “SS” code 00 (zero-zero). Only FEMA designated EAS sources, i.e. PEP stations and IPAWS gateways, are authorized to activate the national EAS using the U.S. “SS” code 00 (zero-zero) and “PSSCCC” = 000000 (six zeros). For the purpose of EAS activations, the entire United States shall include all EAS Participants in all States, the District of Columbia, and any commonwealth, territory, dependency, possession or territorial waters of the United States.

* * * * *

§ 11.32 EAS Encoder.

* * * * *

(5) Originator Daytime, Originator Year and Identification Stamps. The encoder shall affix the Originator Daytime JJJHHMM and Originator Year YYYY automatically to all initial messages, and shall not change them when relaying messages. If the Originator Year YYYY code is missing in a relayed message, the encoder shall not add it. The encoder shall affix the ID Stamp LLLLLLLL codes automatically to all messages transmitted and re-transmitted.

* * * * *

§ 11.33 EAS Decoder.

(a) * * *

(9) *Reset*. There shall be methods to automatically and manually reset the decoder to the normal monitoring condition. Operators shall be able to select a time interval, not less than two minutes, in which the decoder will automatically reset if it received an EAS header code but not an end-of-message (EOM) code. Messages received with the EAN Event code shall not automatically reset prior to the time interval specified by the header code Valid Time period +TTTT, so that lengthy Presidential messages can be handled. The last message received with valid header codes shall be displayed as required by paragraph (a)(4) of this section before the decoder is reset.

(10) *Message Validity*. Decoders shall provide reception error detection and validation of the header codes of each received message to ascertain if the message is valid. Header code comparisons may be accomplished through the use of a bit-by-bit compare or any other error detection and validation protocol. A header code shall only be considered valid when two of the three headers match exactly, and syntactically well formed as specified in §11.31(c).

(11) *EAN override*. A header code with the Primary Entry Point System (PEP) Originator code specified in §11.31(d), Emergency Action Notification (EAN) Event code specified in §11.31(e), and includes one or more Location Codes for the entire United States (000000) or preselected State or State/county specified in §11.31(f) that is received through any of the inputs shall override all other messages.

(12) *Automatic relay*. Decoders shall not automatically relay messages, including EAN messages, unless the header code passes all of the following checks:

(i) ID Stamp (LLLLLLL) code matches one of the assigned monitoring sources (i.e. unexpected input source),

(ii) Not a duplicate of a recent message, as specified in § 11.33(a)(3)(ii), ignoring the ID Stamp (LLLLLLLL) code, (i.e. duplicate message),

(iii) Originator Daytime (JJJHHMM) and, if present, Originator Year (YYYY) is not more than 15 minutes in the future (i.e. clock skew too great), and

(iv) Originator Daytime (JJJHHMM) and, if present, Originator Year (YYYY) is not more than the Valid Time period (+TTTT) in the past (i.e. message expired).

(13) *Multiple messages*. While receiving a message on an input, decoders shall treat receipt of valid header codes different from the current message from the same input as a missing end-of-message (EOM), shall properly end the current message (i.e. transmit a EOM), and start processing a new message. Decoders shall treat receipt of header codes matching the current message from the same input as extraneous echoes during the message, and not the end-of-message (EOM) for the current message.

* * * * *

§ 11.34 Acceptability of the equipment.

* * * * *

(d) Manufacturers must include instructions and information on how to install, operate and program an EAS Encoder, EAS Decoder, or combined unit and a list of all State and county ANSI numbers with each unit sold or marketed in the U.S. A single summary, chapter or manual in the user documentation shall describe the security mechanisms provided, guidelines on their use, and how they interact with one another.

* * * * *

(h) The security mechanisms of the EAS Encoder, EAS Decoder, or combined unit shall be tested and found to work. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security mechanisms in the initial, default out-of-the-box configuration based on the manufacturer’s security guidance. Installation instructions shall provide security guidance for the initial, default out-of-the-box configuration and security cautions. The manufacturer’s guidance may be based on a basic and simplistic security policy for common network architectures. EAS Participants are responsible for implementing their specific security policies to maintain equipment operational readiness as specified in §11.35.

* * * * *

§ 11.35 Equipment operational readiness.

* * * * *

(d) EAS Participants are responsible for security policies ensuring and monitoring the security of their EAS devices and attached systems, detecting and mitigating unauthorized access, and remediating identified vulnerabilities. Participants should design multiple layers of security controls to establish several lines of defense. At the minimum, participants shall ensure the following:

(1) *Protect against unauthorized* access. Change default passwords and settings for EAS devices and system-based credentials. Implement an adequate password policy (i.e. require strong, complex passwords) and/or multifactor authentication protocols. Monitor logs for use of credentials, and promptly terminate unauthorized, unused or unwarranted credentials.

(2) *Defense in depth*. Implement defense in depth security practices, e.g. network segmentation, segregation and firewalls; to protect EAS devices and attached systems from direct access through the Internet and external connections outside the direct control of the EAS participant. Only use secure connections when remotely accessing EAS devices and attached systems.

(3) *Remediate identified vulnerabilities.* Security updates and patches for EAS devices and attached systems are installed in an expeditious manner. If a manufacturer no longer supports a device or system, participants shall implement alternative measures reasonably sufficient to manage the risk of unsupported devices and systems.

(4) *Incident response plan.* Have an incident response plan. If an incident is discovered, there should be a quick risk assessment performed to evaluate the effect of both the attack and the options to respond. Participants follow the recordkeeping and reporting procedures for defective equipment in paragraphs (b) and (c) of this section when implementing the response.

(5) *CAP digital signature validation*. EAS devices and attached systems are configured to validate digital signatures on CAP messages when the source of the CAP message includes this feature. Digital signature verification keys and certificate authorities are updated when revoked or expired.

* * * * *

§11.52 EAS code and Attention Signal Monitoring requirements.

(a) EAS Participants must install and operate during their hours of operation, equipment that is capable of receiving and processing emergency messages in the EAS Protocol and the Common Alerting Protocol. The Attention Signal will not be used to actuate two-tone decoders but will be used as an aural alert signal.

(b) If manual interrupt is used as authorized in paragraph (e)(2) of this section, decoders must be located so that operators at their normal duty stations are alerted immediately when EAS messages with preselected codes are received.

(c) EAS Participants that are co-owned and co-located with a combined studio or control facility (such as an AM and FM licensed to the same entity and at the same location or a cable headend serving more than one system) may comply with the EAS monitoring requirements contained in this section for the combined station or system with one EAS Decoder. The requirements of §11.33 must be met by the combined facility.

(d) EAS Participants must comply with the following monitoring requirements:

(1) With respect to monitoring for EAS messages distributed using the EAS Protocol, EAS Participants must monitor two key EAS sources designated to distribute the Presidential Alert.

(2) With respect to monitoring for EAS messages distributed using the Common Alerting Protocol (CAP), EAS Participants must interface with the Federal Emergency Management Agency's Integrated Public Alert and Warning System (IPAWS).

(3) If the required EAS message sources cannot be received, alternate arrangements or a waiver may be obtained by written request to the Chief, Public Safety and Homeland Security Bureau. In an emergency, a waiver may be issued over the telephone with a follow up letter to confirm temporary or permanent reassignment.

(4) Decoders must be programmed with the mandatory Emergency Action Notification (EAN), National Periodic Test (NPT), National Information Center (NIC), Required Monthly Test (RMT) and Required Weekly (RWT) event codes; the appropriate originator codes; and accompanying U.S., State and State/county location codes.

(e) EAS Participants must interrupt normal programming either automatically or manually when they receive a valid national EAS message from the Primary Entry Point System (PEP) originator code with the Emergency Action Notification (EAN) or National Periodic test (NPT) event code and including the U.S. or their State or State/county location code; or a valid State/local EAS message with the Required Monthly Test (RMT) event code and including their State or State/county location code.

(1) Automatic interrupt of programming and transmission of the EAS message is required when facilities are unattended. Automatic operation must provide a permanent record of the EAS message that contains at a minimum the following information: Originator, Event, Location(s) and valid time period of the message.

(2) Manual interrupt of programming and transmission of the EAS message may be used. Emergency Action Notification (EAN) and National Periodic Test (NPT) messages must be transmitted immediately. Required Monthly Test (RMT) messages must be transmitted within 60 minutes. All actions must be logged and recorded.

* * * * *

§11.61 Tests of EAS procedures.

(a) EAS Participants shall transmit required tests of the EAS as follows:

(1) Required Monthly Tests of the EAS.

(i) All EAS Participants shall participate in required monthly tests of the EAS scheduled by the State/Local Emergency Communications Committee for their Local EAS Area or State. These tests shall use the event code RMT.

(ii) The testing schedule, script content, location codes and designated alert sources will be developed by State/Local Emergency Communications Committees in cooperation with affected EAS Participants. Only the designated alert sources shall initiate required monthly tests. Over the course of the year, SECCs/LECCs should schedule monthly tests through different EAS entry points so all designated alert sources are tested. Tests shall include the State or State/county location codes for the designated testing area. Tests in odd numbered months shall occur between 8:30 a.m. and local sunset. Tests in even numbered months shall occur between local sunset and 8:30 a.m.

(iii) Valid tests must be transmitted within 60 minutes of receipt by EAS Participants when the accompanying location codes include their State or State/county. The transmission must include the EAS header codes, Attention Signal, Test Script and EOM codes; and comply with the audio and visual message requirements in §11.51.

(iv) These tests are not required during the month that a national periodic test is conducted.

(v) EAS participants not required to have equipment capable of generating the EAS codes, as specified in §11.51(e), are required to transmit only the test script.

(vi) On multi-channel systems, EAS Participants may comply with this test by performing these tests on at least one of the most available, consistent and reliable channels accessible to the general public or all subscribers; and on at least 10% of all programmed channels monthly (excluding local-into-local channels for which the monthly tests are passed through by the multi-channel provider), with channels tested varying from month to month, so that over the course of a given year, 100% of all programmed channels are tested.

(2) Required Weekly Tests of the EAS.

(i) All EAS Participants shall transmit required weekly tests at scheduled or random days and times each week. These tests shall use the event code RWT. Additional tests may be performed anytime on any channel(s).

(ii) EAS Participants must include the state and county location codes for the community of license or location of the EAS Participant. Other State or State/county location codes in the participant's service area may be included.

(iii) The transmission must include the EAS header and EOM codes; and comply with the audio message requirements in §11.51.

(iv) These tests are not required during the week that a national periodic test or required monthly test is conducted.

(v) EAS Participants are not required to transmit a visual message when transmitting this test. When specified in §11.11(a), those EAS Participants are not required to cause the video interrupt and audio alert message on all channels during this test.

(vi) EAS participants not required to have equipment capable of generating the EAS codes, as specified in §11.51(e), are not required to transmit this test; but must log receipt, as specified in §11.35(a).

(vii) On multi-channel systems, EAS Participants may comply with this test by performing these tests on at least one of the most available, consistent and reliable channels accessible to the general public or all subscribers.

(3) National Periodic Tests of the EAS.

(i) All EAS Participants shall participate in national periodic tests as scheduled by the Commission in consultation with the Federal Emergency Management Agency (FEMA). These tests shall be activated through FEMA designated test sources. These tests shall use the event code NPT; and the U.S. or State or State/county location codes for the testing area. Notice shall be provided to EAS Participants by the Commission at least two months prior to the conduct of any such test.

(ii) Valid tests must be transmitted immediately upon receipt by EAS Participants when the accompanying location codes include the U.S. or their State or State/county. The transmission must comply with the audio and visual message requirements in §11.51.

(iii) Transmitting EAS emergency messages may take priority over transmitting this test.

(iv) Test results as required by the Commission shall be logged by all EAS Participants into the EAS Test Reporting System (ETRS) as determined by the Commission's Public Safety and Homeland Security Bureau, subject to the following requirements:

(A) EAS Participants shall provide the identifying information required by the ETRS initially no later than sixty days after the publication in the Federal Register of a notice announcing the approval by the Office of Management and Budget of the modified information collection requirements under the Paperwork Reduction Act of 1995 and an effective date of the rule amendment, or within sixty days of the launch of the ETRS, whichever is later, and shall renew this identifying information on a yearly basis.

(B) “Day of test” data shall be filed in the ETRS by the end of the next business day after these tests or as otherwise required by the Public Safety and Homeland Security Bureau.

(C) Detailed post-test data shall be filed in the ETRS within forty-five (45) days following these tests.

(4) EAS activations in lieu of required monthly and weekly tests.

(i) Transmitting EAS activations for emergencies or exercises using live event codes may replace transmitting a monthly or weekly tests required by this section. To substitute for a monthly test in paragraph (a)(1) of this section, the activation must include transmission of the EAS header codes, Attention Signal, audio message and EOM code and comply with the visual message requirements in §11.51. To substitute for the weekly test in paragraph (a)(2) of this section, the activation must include transmission of the EAS header and EOM codes.

(5) Practice/Demo Warning tests of the EAS.

(i) EAS Participants may transmit practice/demo warning tests at any time on any channel(s). These tests shall use the event code DMO.

(ii) This test is not an acceptable substitute for required monthly or weekly tests in paragraph (4) above.

(iii) EAS Participants in cooperation with local authorities as part of a local written agreement, may conduct this test in a specific local authorities’ area. EAS

Participants should coordinate with local authorities so tests by one or multiple local authorities which impact the public in the same, overlapping or nearby areas are no more intrusive or disruptive than required monthly tests in paragraph (1) above.

(b) Entries shall be made in EAS Participant records, as specified in §11.35(a) and 11.54(a)(3).

(c) Special EAS tests at the state and local levels using the standard test event codes DMO, RMT and RWT may be performed anytime following procedures in Local EAS Area and State plans.

(d) Non-geographic EAS Participants, including DBS and SDARS, shall comply with this section by choosing a state and county location. Non-geographic EAS Participants shall monitor their chosen State/county EAS and CAP primary sources to participate in required monthly, weekly and national tests.

§11.62 EAS exercises.

(a) Live Code Drills may be conducted using live event codes instead of standard test codes to exercise the EAS and raise public awareness, provided that the governmental entity conducting the exercise:

   (1) Notifies the Commission at least two months prior to the conduct of any such Live Code Drill;

   (2) Coordinates with the EAS and governmental points of contact for the planned exercise area and adjacent Local EAS Areas or States to avoid conflicting Live Code Drills within one month before and after the scheduled exercise;

   (3) Engages in outreach throughout the 30 days prior to the exercise among EAS Participants, local and state emergency authorities, first responder organizations including Public Safety Answering Points (PSAPs), news media and the public in the planned exercise area and adjacent EAS areas in order to notify them that live event codes will be used, but that no emergency is in fact occurring;

   (4) Provides notification in accessible formats during the Live Code Drill (e.g., audio voiceovers and video crawls as described in §11.51) to make sure the public understands that the Live Code Drill is not, in fact, warning about an actual emergency;

   (5) And has a contingency plan in case an actual or potential emergency which may require the use of the EAS occurs during the scheduled exercise.

C. Protocol Testing Examples

In the following examples, EAS headers may extend across multiple lines. EAS transmissions do not have line breaks. ID Stamps are fictional or government agencies, any resemblance to other organizations is purely coincidental.

C.1. EAS Verification and Validation Testing

Verification is intended to check that a product, service, or system (or portion thereof, or set thereof) meets a set of design specifications. Validation is intended to ensure a product, service, or system (or portion thereof, or set thereof) results in a product, service, or system (or portion thereof, or set thereof) that meets the operational needs of the user. The following are samples of valid EAS protocol messages.

C.1.1. Required Weekly Test (RWT)

A hypothetical EAS protocol transmission for a Required Weekly Test on October 7, 2015.

```
[PREAMBLE]ZCZC-EAS-RWT-024033+0100-2801723-RADIO/FM-2015-
(one second pause)
[PREAMBLE]ZCZC-EAS-RWT-024033+0100-2801723-RADIO/FM–2015-
(one second pause)
[PREAMBLE]ZCZC-EAS-RWT-024033+0100-2801723-RADIO/FM-2015-
(NO Attention Tone Transmitted)
(NO Audio Message Transmitted)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Required Weekly Test (RWT) issued at the request of an EAS participant (EAS) for the Maryland county of Prince George’s (024033) at 1:23 pm EST (1723 UTC) on October 7, 2015 (280th day of the current year) until 2:23 pm EST (+0100) transmitted by RADIO-FM. The transmission does not include either an Attention Signal or audio message.

Each EAS participant must transmit a Required Weekly Test each week. Receipt of a RWT transmission must be logged and not re-transmitted by other EAS participants.

C.1.2. Required Monthly Test (RMT)

A hypothetical EAS protocol transmission for a Required Monthly Test on January 20, 2016.

```
[PREAMBLE]ZCZC-EAS-RMT-011001-024021-024031-024033-051510-
051013-051059-051600-051610-051061-051107-051683-051685-
051153-051179+0100-0201545-CableUS -2016-
(one second pause)
```

```
[PREAMBLE]ZCZC-EAS-RMT-011001-024021-024031-024033-051510-
051013-051059-051600-051610-051061-051107-051683-051685-
051153-051179+0100-0201545-CableUS -2016-
(one second pause)
[PREAMBLE]ZCZC-EAS-RMT-011001-024021-024031-024033-051510-
051013-051059-051600-051610-051061-051107-051683-051685-
051153-051179+0100-0201545-CableUS -2016-
(one to three second pause)
(transmission of 8 to 25 seconds of Attention Signal)
(one to three second pause)
(brief audio message describing the test, up to two
minutes)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Required Monthly Test (RMT) issued at the request of an EAS Participant (EAS) for the District of Columbia (011001); the Maryland counties of Frederick (024021), Montgomery (024031) and Prince George’s (024033); the Virginia counties of Arlington (051013), Fairfax (051059), Fauquier (051061), Loudoun (051107), Prince Willian (051153) and Stafford (051179); the Virginia cities of Alexandria (051510), Fairfax (051600), Falls Church (051610), Manassas (051683) and Manassas Park (051685) at 10:45 am EST (1545 UTC) on January 20, 2016 (20th day of the year 2016) until 11:45 am EST (+0100) transmitted by Cable US. The transmission includes the Attention Signal and brief audio message.

Only designated originators as coordinated in the State/local EAS plan should initiate Required Monthly Tests.

Upon receipt of a valid RMT message affecting the Local EAS Area of the EAS Participant, as designated in the State/Local EAS Plan, EAS Participants must interrupt programming and relay the EAS message within 60 minutes. A valid EAS message must have an expected transmission ID Stamp, must not be a duplicate, must not be too far in the future and must not be expired.

C.1.3. Winter Storm Warning (WSW)

A hypothetical Weather Radio SAME protocol transmission for a Winter Storm Warning on January 21, 2016.

```
[PREAMBLE]ZCZC-WXR-WSW-051043-054037+0600-0211709-KLWX/NWS-
(one second pause)
[PREAMBLE]ZCZC-WXR-WSW-051043-054037+0600-0211709-KLWX/NWS-
(one second pause)
[PREAMBLE]ZCZC-WXR-WSW-051043-054037+0600-0211709-KLWX/NWS-
(one to three second pause)
```

```
(transmission of 1050 Hz Warning Alarm Tone for 8 to 10
Seconds)
(three to five second pause)
(brief audio message describing the weather alert, up to
two minutes)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Winter Storm Warning (WSW) issued at the request of the National Weather Service (WXR) for the Virginia county of Clarke (051043); and the West Virginia county of Jefferson (054037) at 12:09 pm EST (1709 UTC) on January 21, 2016 (21st day of the current year) until 6:09 pm EST (+0600) transmitted by KLWX/NWS.

The Weather Radio SAME Protocol is compatible, but not identical to EAS Protocol transmissions. WRSAME uses a 1050 Hz Warning Alarm Tone, and does not include the Originator Year (YYYY). EAS participants should remove the WRSAME Warning Alarm Tone and use the EAS Attention Signal. They should not add the Originator Year (YYYY) when re-transmitting a message received without the YYYY protocol element.

Upon receipt of a valid WRSAME message, EAS Participants may interrupt programming and relay the message using the EAS Protocol. A valid EAS message must have an expected transmission ID Stamp, must not be a duplicate, must not be too far in the future and must not be expired.

C.1.4. Child Abduction Emergency (CAE) – AMBER Alert

A hypothetical EAS protocol transmission for AMBER alert on February 7, 2016.

```
[PREAMBLE]ZCZC-CIV-CAE-051000+1200-0381923-ZETA FM -2016-
(one second pause)
[PREAMBLE]ZCZC-CIV-CAE-051000+1200-0381923-ZETA FM -2016-
(one second pause)
[PREAMBLE]ZCZC-CIV-CAE-051000+1200-0381923-ZETA FM -2016-
(one to three second pause)
(transmission of 8 to 25 seconds of Attention Signal)
(one to three second pause)
(brief audio message describing the AMBER alert, up to two
minutes)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
```

```
[PREAMBLE]NNNN
```

This is an example of an AMBER Alert, Child Abduction Emergency (CAE) issued at the request of a Civil Authority (CIV) for the entire Commonwealth of Virginia (051000) at 2:23 pm EST (1923 UTC) on February 7, 2016 (38th day of the year 2016) until 2:23 am EST (+0600) on February 8, 2016 transmitted by ZETA-FM. The transmission includes the Attention Signal and brief audio message.

Upon receipt of a valid message, EAS Participants may interrupt programming and relay the message using the EAS Protocol. A valid EAS message must have an expected transmission ID Stamp, must not be a duplicate, must not be too far in the future and must not be expired.

C.1.5. Nation-wide Presidential Alert (EAN)

A hypothetical EAS protocol transmission for an Emergency Action Notification (EAN) on November 9, 2017.

```
[PREAMBLE]ZCZC-PEP-EAN-000000+0015-3131900-SAT/PEP -2017-
(one second pause)
[PREAMBLE]ZCZC-PEP-EAN-000000+0015-3131900-SAT/PEP -2017-
(one second pause)
[PREAMBLE]ZCZC-PEP-EAN-000000+0015-3131900-SAT/PEP -2017-
(one to three second pause)
(transmission of 8 to 25 seconds of Attention Signal)
(one to three second pause)
(audio message from the President, up to +TTTT
hours/minutes)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Presidential Alert (EAN) issued at the request of National Authorities (PEP) for the entire United States (000000) at 2:00 pm EST (1900 UTC) on November 9, 2017 (313rd day of the year 2016) until 2:15 pm EST (+0015) transmitted by SAT/PEP. The transmission includes the Attention Signal and a “live” audio message up to 15 minutes long, ending with the EOM (NNNN).

Upon receipt of a valid EAN message affecting the entire United States (000000), EAS Participants must immediately interrupt programming. relay the complete Presidential message using the EAS Protocol from the beginning of the audio message until the end-of-message (EOM), or the Valid Time interval (e.g. +0015 = 15 minutes) elapses. The input audio sources are not joined “in progress,” several seconds after transmitting the EAS Header and Attention Signal. Instead, EAS devices should buffer the “live” audio while transmitting the EAS Header and Attention Signal, and continue streaming the “live” audio message from the buffer.

Nevertheless, EAS Participants are permitted to transmit any other source of the President's audio message instead of the EAS audio feed, such as a broadcast network feed.

A valid EAN message must be originated by the Primary Entry Point System (PEP), must have an expected transmission ID Stamp, must not be a duplicate, must not be too far in the future and must not be expired.

C.1.6. Nation-wide National Periodic Test (NPT)

A hypothetical EAS protocol transmission for a National Periodic Test (NPT) on December 31, 2016.

```
[PREAMBLE]ZCZC-PEP-NPT-000000+0600-3662400-FEMA AOC-2016-
(one second pause)
[PREAMBLE]ZCZC-PEP-NPT-000000+0600-3662400-FEMA AOC-2016-
(one second pause)
[PREAMBLE]ZCZC-PEP-NPT-000000+0600-3662400-FEMA AOC-2016-
(one to three second pause)
(transmission of 8 to 25 seconds of Attention Signal)
(one to three second pause)
(brief audio message describing the test, up to two
minutes)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a National Periodic Test issued at the request of National Authorities (PEP) for the entire United States (000000) at 7:00 pm EST (2400 UTC) on December 31, 2016 (366th day of the year 2016, a leap year) until 1:00 am EST (+0600) on January 1, 2017 transmitted by FEMA AOC. The transmission includes the Attention Signal and brief audio message. The time representation 2400 is valid according to ISO 8691, "Data elements and interchange formats – Information interchange – Representation of dates and times ". The notation 0000 refers to the beginning of a calendar day, and 2400 refers to the end of a calendar day. Most 24-hour clocks use 0000 to 2359, but EAS decoders should be prepared to handle clock times including 2400 Midnight.

A valid nation-wide (000000) message must be originated by the Primary Entry Point System (PEP), must have an expected transmission ID Stamp, must not be a duplicate, must not be too far in the future and must not be expired.

C.1.7. New and Deprecated Location Codes

A hypothetical Weather Radio SAME protocol transmission for a Winter Storm Warning on January 21, 2016 with new and deprecated location codes.

```
[PREAMBLE]ZCZC-WXR-WSW-046102-046113+0600-0211709-KUNR/NWS-
(one second pause)
[PREAMBLE]ZCZC-WXR-WSW-046102-046113+0600-0211709-KUNR/NWS-
(one second pause)
[PREAMBLE]ZCZC-WXR-WSW-046102-046113+0600-0211709-KUNR/NWS-
(one to three second pause)
(transmission of 1050 Hz Warning Alarm Tone for 8 to 10
Seconds)
(three to five second pause)
(brief audio message describing the weather alert, up to
two minutes)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Winter Storm Warning (WSW) issued at the request of the National Weather Service (WXR) for the South Dakota county of Oglala Lakota (046102) and Shannon County (046113) at 10:09 pm MST (1709 UTC) on January 21, 2016 (21st day of the current year) until 4:09 pm MST (+0600) transmitted by KUNR/NWS.

This example contains new and deprecated ANSI (FIPS) codes for Oglala Lakota County, formerly known as Shannon County, in South Dakota. In this instance, the geographic area remained the same, but the ANSI (FIPS) code was changed to reflect the new name. Occasionally the U.S. Census bureau updates ANSI (FIPS) State/county codes and the National Weather Service updates marine codes to reflect name and geographic changes.

EAS operators should be able to add new codes and change the translation of existing codes in EAS devices. Deprecated codes usually are not removed immediately to support a transition period while both codes may be used. EAS devices should not reject EAS messages containing both defined and unknown/undefined location code, because the EAS device may not have been updated with recently added or changed location. If the EAS message with unknown/undefined location codes is selected for relaying, the EAS device must not change the EAS header codes. It must relay the exact EAS header intact, except the ID Stamp, including all known and unknown/undefined location codes in the EAS header.

Although all current FCC authorized location codes are numeric, the EAS protocol could allow upper and lowercase alphabetic and other printable ASCII characters, except the plus sign and hyphen, as code values. For compatibility with the SAME protocol and robustness, EAS decoders should be prepared for location codes with any printable ASCII characters.

C.1.8. New Event Codes

A hypothetical Weather Radio SAME protocol transmission for a new Wild Weather Warning on January 27, 2016.

```
[PREAMBLE]ZCZC-WXR-WWW-073535+0600-0271715-KLWX/NWS-
(one second pause)
[PREAMBLE]ZCZC-WXR-WWW-073535+0600-0271715-KLWX/NWS-
(one second pause)
[PREAMBLE]ZCZC-WXR-WWW-073535+0600-0271715-KLWX/NWS-
(one to three second pause)
(transmission of 1050 Hz Warning Alarm Tone for 8 to 10
Seconds)
(three to five second pause)
(brief audio message describing the weather alert, up to
two minutes)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Wild Weather Warning (WWW) issued at the request of the National Weather Service (WXR) for the Tidal Potomac from Key Bridge to Indian Head MD (073535) at 12:15 pm EST (1715 UTC) on January 27, 2016 (27th day of the current year) until 6:15 pm EST (+0600) transmitted by KLWX/NWS.

Wild Weather Warning (WWW) is an imaginary event code which could be defined in the future. EAS operators should be able to add new event codes and change the translation of existing codes in EAS devices. Deprecated event codes usually are not removed immediately, e.g. Emergency Action Termination (EAT), but no longer used. EAS Participants should not transmit new EAS event codes in messages until defined by the FCC. But EAS devices should be able to handle new EAS event codes when added by the operator.

The National Weather Service SAME protocol includes several additional event codes, beyond those defined by the FCC, such as Transmitter Carrier Off (TXF), Transmitter Carrier On (TXO), Transmitter Backup On (TXB), Transmitter Primary On (TXP). EAS decoders may log unknown or undefined event codes for diagnostic and operator information, or the operator may choose to ignore unknown and undefined event codes.

Although all current FCC authorized event codes are uppercase alphabetic characters, the EAS protocol could allow lowercase alphabetic and other printable ASCII characters, except the plus sign and hyphen, as code values. For compatibility with the SAME protocol and robustness, EAS decoders should be prepared for event codes with any printable ASCII characters.

C.1.9. Practice/Demo Event Codes

A hypothetical Weather Radio SAME protocol transmission for a Practice/Demo Warning on June 4, 2015.

```
[PREAMBLE]ZCZC-WXR-DMO-999000+0030-1561634-KLWX/NWS-
(one second pause)
[PREAMBLE]ZCZC-WXR-DMO-999000+0030-1561634-KLWX/NWS-
(one second pause)
[PREAMBLE]ZCZC-WXR-DMO-999000+0030-1561634-KLWX/NWS-
(one to three second pause)
(transmission of 1050 Hz Warning Alarm Tone for 8 to 10
Seconds)
(three to five second pause)
(brief audio message describing the weather alert, up to
two minutes)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Practice/Demo Warning (DMO) issued at the request of the National Weather Service (WXR) for an undefined area (999000) at 12:34 pm EDT (1634 UTC) on June 4, 2015 (156th day of the current year) until 1:04 pm EST (+0030) transmitted by KLWX/NWS.

The event code "DMO" should not normally be programmed into receivers or EAS decoder, and the location code of "999000" does not match any existing or future geographical area codes. Its primary use is to provide EAS Participants a means of conducting exercises to practice issuing authentic warnings and other critical messages without disrupting the EAS network or turning on industrial and general public receiver decoders, unless optionally selected by the user.

C.2. EAS Robustness Testing

ANSI and IEEE have defined robustness as the degree to which a system or component can function correctly in the presence of invalid inputs or stressful environmental conditions. Robustness testing is any quality assurance methodology focused on testing the robustness of software. The following EAS messages are samples of EAS protocol robustness tests.

C.2.1. Mixed-case Required Weekly Test (RWT)

A hypothetical EAS protocol transmission for a Required Weekly Test on October 7, 2015.

```
[PREAMBLE]ZCZC-eAa-rWt-024033+0100-2801723-Radio/FM-2015-
(one second pause)
[PREAMBLE]ZCZC-eAa-rWt-024033+0100-2801723-Radio/FM–2015-
```

```
(one second pause)
[PREAMBLE]ZCZC-eAs-rWt-024033+0100-2801723-Radio/FM-2015-
(NO Attention Tone Transmitted)
(NO Audio Message Transmitted)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Required Weekly Test (RWT) issued at the request of an EAS participant (EAS) for the Maryland county of Prince George's (024033) at 1:23 pm EST (1723 UTC) on October 7, 2015 (280th day of the current year) until 2:23 pm EST (+0100) transmitted by RADIO-FM. The transmission does not include either an Attention Signal or audio message.

In this instance, the Originator Code and Event Code consist of the mixed-case codes "eAs" and "rWt". The codes do not match the pre-selected upper-case codes "EAS" and "RWT". The ID Stamp uses case-sensitive LLLLLLLL identification stamps. The ID Stamp should exactly match the expected transmission identifier for the source.

C.2.2. Incomplete End of Message (EOM) Codes

A hypothetical EAS protocol transmission for a Required Weekly Test on October 7, 2015 with an incomplete EOM.

```
[PREAMBLE]ZCZC-EAS-RWT-024033+0100-2801723-RADIO/FM-2015-
(one second pause)
[PREAMBLE]ZCZC-EAS-RWT-024033+0100-2801723-RADIO/FM–2015-
(one second pause)
[PREAMBLE]ZCZC-EAS-RWT-024033+0100-2801723-RADIO/FM-2015-
(NO Attention Tone Transmitted)
(NO Audio Message Transmitted)
(one to three second pause)
[PREAMBLE]NNNN
```

This is an example of a Required Weekly Test (RWT) issued at the request of an EAS participant (EAS) for the Maryland county of Prince George's (024033) at 1:23 pm EST (1723 UTC) on October 7, 2015 (280th day of the current year) until 2:23 pm EST (+0100) transmitted by RADIO-FM. The transmission does not include either an Attention Signal or audio message.

In this instance, only one EOM (NNNN) data burst is detected. An EOM can be considered valid if the decoder detects the preamble followed by at least one N, but preferably two (2) N's. The preamble and any number of N's will never be sent except at the end of the message.

C.2.3. Only End of Message (EOM) Codes

A hypothetical EAS protocol transmission with only EOM Codes.

```
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

In this instance, only EOM (NNNN) data bursts are detected. This may be a recording of only of the EOM to clear the EAS system due to an EAS encoder malfunction, or the beginning of the EAS message was missed due to transmission or reception problems.

When processing an EAS message, an EOM can be considered valid if the decoder detects the preamble followed by at least one N, but preferably two (2) N's. The preamble and any number of N's will never be sent except at the end of the message.

When not processing an EAS message, most EAS decoders ignore extraneous EOM transmissions. EAS decoders may log unexpected EOM Codes for diagnostic and operator information

C.2.4. Duplicate Interstitial EAS Headers

A hypothetical EAS protocol transmission, with duplicate EAN headers on November 9, 2017.

```
[PREAMBLE]ZCZC-PEP-EAN-011001+0015-3131900-AFED    -2017-
(one second pause)
[PREAMBLE]ZCZC-PEP-EAN-011001+0015-3131900-AFED    -2017-
(one second pause)
[PREAMBLE]ZCZC-PEP-EAN-011001+0015-3131900-AFED    -2017-
(one to three second pause)
(transmission of 8 to 25 seconds of Attention Signal)
(one to three second pause)
(initial portion of audio message from the President)
[PREAMBLE]ZCZC-PEP-EAN-011001+0015-3131900-BFED    -2017-
(one second pause)
[PREAMBLE]ZCZC-PEP-EAN-011001+0015-3131900-BFED    -2017-
(one second pause)
[PREAMBLE]ZCZC-PEP-EAN-011001+0015-3131900-BFED    -2017-
(remainder of audio message from the President)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Presidential Alert (EAN) issued at the request of National Authorities (PEP) for the District of Columbia at 2:00 pm EST (1900 UTC) on November 9, 2017 (313rd day of the year 2016) until 2:15 pm EST (+0015) transmitted by AFED and BFED. The transmission includes the Attention Signal and a “live” audio message up to 15 minutes (+0015) long, ending with the EOM (NNNN).

During the EAN message, duplicate EAS headers are detected when feedback from multiple transmitters are bridged together. A human operator may decide to abort the EAN message due to audio issues. Automated, unattended equipment should err on the side of the message may still be semi-intelligible or the audio may improve upstream.

C.2.5. Different Interstitial EAS Headers

A hypothetical WRSAME protocol transmission interrupted by a different EAS protocol transmission on March 24, 2017.

```
[PREAMBLE]ZCZC-WXR-TSW-002000+0100-0831744-OOPS/NWS-
(one second pause)
[PREAMBLE] ZCZC-WXR-TSW-002000+0100-0831744-OOPS/NWS-
(one second pause)
[PREAMBLE] ZCZC-WXR-TSW-002000+0100-0831744-OOPS/NWS-
(one to three second pause)
(transmission of 1050 Hz Warning Alarm Tone for 8 to 10
Seconds)
(three to five second pause)
(brief audio message describing the tsunami warning, up to
two minutes)
[PREAMBLE]ZCZC-CIV-EVI-002110+0100-0831745-OOPS/EMA -
(one second pause)
[PREAMBLE]ZCZC-CIV-EVI-002110+0100-0831745-OOPS/EMA -
(one second pause)
[PREAMBLE]ZCZC-CIV-EVI-002110+0100-0831745-OOPS/EMA -
(one to three second pause)
(transmission of 8 to 25 seconds of Attention Signal)
(one to three second pause)
(brief audio message describing the evacuation, up to two
minutes)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Tsunami Warning issued at the request of the National Weather Service for the entire State of Alaska at 1:44 pm EDT (1744 UTC) on March 24, 2017 (83rd day of the year 2017) until 2:44 pm EST (+0100) transmitted by OOPS/NWS.

During the Tsunami Warning message, different EAS headers are detected: An Immediate Evacuation Warning issued at the request of the Civil Authorities for the Alaska borough of

Juneau at 1:45 pm EDT (1744 UTC) on March 24, 2017 (83rd day of the year 2017) until 2:45 pm EST (+0100) transmitted by OOPS/EMA.

This may occur when separate WRSAME and EAS equipment, or two EAS encoders, is installed in series. One protocol encoder may interrupt the other protocol encoder in mid-transmission. While pre-empting another alert may be considered acceptable, an EAS decoder needs to be able to handle interrupted protocol transmissions.

C.2.6. Clock Problem with EAS Message

A hypothetical EAS protocol transmission for a Required Monthly Test received at 12:00 am EST on February 10, 2016 according to the local clock.

```
[PREAMBLE]ZCZC-CIV-RMT-036005-036047-036061-036081-
036085+0100-0410600-OOPS    -2016-
(one second pause)
[PREAMBLE]ZCZC-CIV-RMT-036005-036047-036061-036081-
036085+0100-0410600-OOPS    -2016-
(one second pause)
[PREAMBLE]ZCZC-CIV-RMT-036005-036047-036061-036081-
036085+0100-0410600-OOPS    -2016-
(one to three second pause)
(transmission of 8 to 25 seconds of Attention Signal)
(one to three second pause)
(brief audio message describing the test, up to two
minutes)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Required Monthly Test (RMT) issued at the request of a Civil Authority for the New York counties of Bronx (036005), Kings (Brooklyn) (036047), New York (Manhattan) (036061), Queens (036081), and Richmond (Staten Island) (036085) at 1:00 am EST (0645 UTC) on February 10, 2016 (41st day of the year 2016) until 2:00 am EST (+0100) transmitted by OOPS. It appears to the EAS decoder as if the message originated 1 hour in the future. A human may apply common sense to decide which clock is correct and manually relay the message, but unattended, automated equipment does not have common sense.

EAS messages are considered “For Immediate Release,” with appropriate equipment hold-off timers and date sanity checks. Messages with origination dates in far past, or far future usually indicate a configuration problem or false message. This is often a local time zone configuration problem, even though EAS messages use Universal Coordinated Time. (UTC). An Originator Daytime in the future may also indicate a very old message for Legacy EAS protocol transmissions, without the Originator Year, since the Day of Year repeats every year. A small amount of clock skew, i.e. 15 minutes, should be tolerated for equipment drift, human variance and disaster resilience.

C.2.7. Invalid Originator of EAN Event Code

A hypothetical EAS protocol transmission for an Emergency Action Notification (EAN) sent instead of a Required Weekly Test on November 9, 2017.

```
[PREAMBLE]ZCZC-EAS-EAN-011001+0015-3131900-OOPS    -2017-
(one second pause)
[PREAMBLE]ZCZC-EAS-EAN-011001+0015-3131900-OOPS   -2017-
(one second pause)
[PREAMBLE]ZCZC-EAS-EAN-011001+0015-3131900-OOPS   -2017-
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Presidential Alert (EAN) issued at the request of a EAS Participant (EAS) for the District of Columbia (011001) at 2:00 pm EST (1900 UTC) on November 9, 2017 (313rd day of the year 2016) until 2:15 pm EST (+0015) transmitted by OOPS.

A valid EAN message must be originated by the Primary Entry Point System (PEP).

This is usually an EAS operator accidently choosing an EAN event code when trying to send a Required Weekly Test or other EAS event. Although EAS equipment may require a confirmation or "lockout" certain codes, human ingenuity to unknowingly defeat safety features can be amazing. EAS decoders will not be able to prevent everything which may happen, basic sanity checks can mitigate the impact.

Only the EAN event code is limited to Primary Entry Point System (PEP) originators. Other national event codes, e.g. NPT and NIC, are expected to be used by national authorities, but are not limited to the PEP origination code.

C.2.8. Invalid Originator of Nation-wide Location Code

A hypothetical EAS protocol transmission for a nation-wide Required Monthly Test sent instead of a State/local RMT on November 9, 2017.

```
[PREAMBLE]ZCZC-EAS-RWT-000000+0015-3131900-OOPS    -2017-
(one second pause)
[PREAMBLE]ZCZC-EAS-RWT-000000+0015-3131900-OOPS   -2017-
(one second pause)
[PREAMBLE]ZCZC-EAS-RWT-000000+0015-3131900-OOPS   -2017-
(one to three second pause)
```

```
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Required Weekly Test (RWT) issued at the request of a EAS Participant (EAS) for the entire United States (000000) at 2:00 pm EST (1900 UTC) on November 9, 2017 (313rd day of the year 2016) until 2:15 pm EST (+0015) transmitted by OOPS.

A message containing a location code with the U.S. “SS” code 00 (zero-zero) must be originated by the Primary Entry Point System (PEP).

This is usually an EAS operator accidently not choosing the correct location when trying to send a Required Weekly Test or other EAS event. Although EAS equipment may require a confirmation or “lockout” certain codes, human ingenuity to unknowingly defeat safety features can be amazing. EAS decoders will not be able to prevent everything which may happen, basic sanity checks can mitigate the impact.

The U.S. “SS” code 00 (zero-zero), with any CCC code or P code, including PSSCCC = 000000 (six zeros), is restricted to Primary Entry Point System (PEP) originators. The U.S. “SS” code 00 (zero-zero) is not limited only to the EAN event code, because other event codes may use nation-wide locations, e.g. NPT and NIC.

C.2.9. Unusual/Undefined U.S. Location Codes

A hypothetical EAS protocol transmission for an Emergency Action Notification (EAN) sent with an undefined U.S. Location Code on November 9, 2017.

```
[PREAMBLE]ZCZC-PEP-EAN-100001+0015-3131910-OOPS    -2017-
(one second pause)
[PREAMBLE]ZCZC-PEP-EAN-100001+0015-3131910-OOPS   -2017-
(one second pause)
[PREAMBLE]ZCZC-PEP-EAN-100001+0015-3131910-OOPS   -2017-
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a Presidential Alert (EAN) issued at the request of National Authorities (PEP) for the United States area of Northwest undefined (100001) at 2:10 pm EST (1910 UTC) on November 9, 2017 (313rd day of the year 2016) until 2:25 pm EST (+0015) transmitted by OOPS.

The U.S. “SS” code 00 (zero-zero) does not define any “CCC” codes besides 000 (zero-zero-zero), i.e. the entire U.S.

ANSI/CEA-2009-B, “Performance Specification for Public Alert Receivers,” specifies a decoder checks the “P” codes = 0 (zero) or 1 to 9; and if “SS” code = 00 (zero-zero), ignores the value of the “CCC” code.

EAS decoders may log undefined/unknown location codes for diagnostic and operator information. If the EAS message does not match any pre-selected location, because all the location codes are unknown/undefined, EAS devices should not relay the message. If an EAS message containing both unknown/undefined location codes and other valid pre-selected location codes is selected for relaying, the EAS device must not change the EAS header codes. It must relay the exact EAS header intact, except the ID Stamp, including all location codes in the EAS header.

The only FCC authorized nation-wide Location Code is PSSCCC = 000000 (six zeros). Regional EAN messages should use SS codes for individual States/territories, and if necessary CCC codes for individual counties/cities within those states/territories, and if necessary P codes for individual portions/subdivisions within those counties/cities or states/territories.

C.2.10. Corrupted Transmission EAS data bursts

A hypothetical EAS protocol transmission corruption for a Required Weekly Test on October 7, 2015.

```
[PREAMBLE]ZCZC-EAS-RWT-024033+ee00-2801723-RADIO/FM-2015-
n6d*6
(one second pause)
[PREAMBLE]ZCZC-EAS-RWT-024033p0100-280xx23-RADIO/FM%jet-
@vhyDF
(one second pause)
[PREAMBLE]ZCZC-EAS-RWT-024033+01nn-2801723-RADIO/FM-2015-
jkTc#5
(NO Attention Tone Transmitted)
(NO Audio Message Transmitted)
(one to three second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
(one second pause)
[PREAMBLE]NNNN
```

This is an example of a corrupted transmission of a Required Weekly Test (RWT) issued at the request of an EAS participant (EAS).

EAS decoders should check that at least two of the three header code transmissions are identical before declaring a match or valid header. The EAS protocol specification allows doing a bit-by-bit check of the three transmissions and attempt to reconstruct a valid code by comparing the bits in each position in each header code transmission and accepting as the valid bit that bit which appears in two of the three header code transmissions. Or EAS decoders may do any other error detection and validation protocol.

In this instance, the EAS two of three headers do not match, some data elements contain invalid values, e.g. letters in time values instead of hours and minutes, one out of three headers is missing the YYYY element, and some extra noise characters. An EAS decoder could attempt to reconstruct a valid header by combining parts of all three headers, or decide they do not match.

C.2.11. Insufficient EAS Headers

A hypothetical EAS protocol transmission for a Required Weekly Test on October 7, 2015 with only one EAS Header.

```
[PREAMBLE]ZCZC-EAS-RWT-024033+0100-2801723-RADIO/FM-2015-
```

This is an example of a Required Weekly Test (RWT) issued at the request of an EAS participant (EAS) for the Maryland county of Prince George’s (024033) at 1:23 pm EST (1723 UTC) on October 7, 2015 (280th day of the current year) until 2:23 pm EST (+0100) transmitted by RADIO-FM. The transmission does not include either an Attention Signal or audio message.

In this instance, only one EAS Header data burst is detected. This may occur because of a very weak signal, too long of a delay between repetitions of the Header data burst, or a recording of a partial EAS message.

An EAS Header should be considered valid only if the decoder detects at least two copies of the Header data burst.

Most EAS decoders ignore extraneous EAS Header transmissions. EAS decoders may log incomplete and unexpected EAS transmissions for diagnostic and operator information.

C.2.12. Transmission Timing Tolerances

A hypothetical EAS protocol transmission for a Required Monthly Test received on February 10, 2016 with two second gaps between data transmissions and long or short inter-audio message gaps.

```
(zero seconds of silence)
[PREAMBLE]ZCZC-CIV-RMT-036005-036047-036061-036081-
036085+0100-0410600-OOPS    -2016-
(two second pause)
[PREAMBLE]ZCZC-CIV-RMT-036005-036047-036061-036081-
036085+0100-0410600-OOPS    -2016-
(two second pause)
[PREAMBLE]ZCZC-CIV-RMT-036005-036047-036061-036081-
036085+0100-0410600-OOPS    -2016-
(zero to six second pause)
(transmission of 4 to 30 seconds of Attention Signal)
(zero to six second pause)
```

```
    (brief audio message describing the test, exactly 120
    seconds)
    (zero to six second pause)
    [PREAMBLE]NNNN
    (two second pause)
    [PREAMBLE]NNNN
    (two second pause)
    [PREAMBLE]NNNN
    (zero seconds of silence)
```

This is an example of a Required Monthly Test (RMT) issued at the request of a Civil Authority for the New York counties of Bronx (036005), Kings (Brooklyn) (036047), New York (Manhattan) (036061), Queens (036081), and Richmond (Staten Island) (036085) at 1:00 am EST (0645 UTC) on February 10, 2016 (41st day of the year 2016) until 2:00 am EST (+0100) transmitted by OOPS.

Timing tolerances should be allowed for variances between hardware and transmission environment. Inter-header gaps may be less or more than one second. The FCC does not specify timing tolerances. Tight tolerances reduce the risk of simulated or false EAS transmissions triggering EAS equipment, too tight tolerances increase the risk valid EAS transmissions will be dismissed as invalid. The SAME protocol specifies 5% (plus or minus) timing tolerances for machine generated Header/EOM transmissions. For compatibility between legacy EAS, SAME and revised EAS with YYYY data elements; EAS decoders should have 10% (plus or minus) timing tolerances for reception of EAS data bursts. EAS encoders should have 2% (plus or minus) timing tolerances for transmission of EAS data bursts.

EAS decoders should not consider lengthy silence as the end of the EAS transmission. Instead they use a two-minute audio limit or EAN +TTTT elapsed timer. However, 30 second audio gaps will often trigger other silence detection equipment in transmission chains. Because EAS equipment is usually installed at the control studio and silence detector equipment at the transmitter site, silence detectors could impact EAS transmissions. 30 second audio gaps in EAS messages are unusual, so this is a low risk. Downstream silence detectors could play a EOM recording when triggered and then its backup programming. More typical is weak audio signals and very quiet audio in EAS messages.

Measuring the two-minute audio time limit is ambiguous depending if it includes the silence at the beginning and end, and the Attention Signal or Warning Alert Signal was accurately detected. Generally audio messages longer than 90 seconds risk being truncated during EAS decoder recording and EAS encoder re-transmission. Likewise, the EAN +TTTT elapsed timer may be triggered during the last 30 seconds, depending on the length of the Attention Signal and beginning of the audio message.